Implementation of Encrypted Visual Cryptographic Shares using RSA Algorithm on FPGA

Ashwini B. M, Y. P. Gowramma

Abstract-The project presents an approach for encrypting visual cryptographically generated image shares using RSA algorithm. The Visual Cryptography Scheme is a secure method that encrypts a secret document or image by breaking it into shares. A distinctive property of Visual Cryptography Scheme is that one can visually decode the secret image by superimposing shares without computation. By taking the advantage of this property, third person can easily retrieve the secret image if shares are passing in sequence over the network. RSA algorithm is used for providing the double security of secret document. The RSA is a new method to encrypt the data by using private and public keys. Thus secret share are not available in their actual form for any alteration by the adversaries who try to create fake shares. The scheme provides more secure secret shares that are robust against a number of attacks & the system provides a strong security for the handwritten text, images and printed documents over the public network. Field Programmable Gate Arrays (FPGAs) are widely used to implement special purpose processors. FPGAs are economically cheaper for low quantity production because its function can be directly reprogrammed by end users. The aim of this project is to design a hardware on which we can encrypt/decrypt a confidential data using visual cryptography and RSA algorithm. in order to reduce the hardware consumption, here I have designed the FPGA such that, we can encrypt the part of the image at a time and we are going to repeat the process until all pixels are encrypted/decrypted.

Keywords- Visual Cryptography; Encryption; Information Security; VCshares

I. INTRODUCTION

In today's information age, information sharing and transfer has increased exponentially. The threat of an intruder accessing secret information has been an ever existing concern for the data communication experts. With the rapid advancement of network topology, multimedia information is transmitted over the Internet conveniently. Various confidential data such as military maps and commercial identification are transmitted over the Internet. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over public network to steal information that they want. To deal with security problems of secret images, we should develop some secure appropriate algorithm by which we can secure our data on internet. With this system visual information (pictures) can be secure over the internet with the help of Visual Cryptography.

Manuscript Received on May 09, 2015.

Ashwini B. M, M.Tech IV Sem, Kalpataru Institute of Technology, Tiptur, Karnataka, India.

Dr. Y. P. Gowramma, Prof. and HOD of Department of CS & E, Kalpataru Institute of Technology, Tiptur, Karnataka, India.

The proposed scheme combines the advantages of both Visual Cryptography as well as Public Key Cryptography. This scheme enhances the security of VC shares by encrypting with Public Key Cryptography [14][15], which provides the strong security to the transfer of secret information in form of images, printed text and hand written material. Visual Cryptography (VC) is a special encryption technique used to encrypt images in such a way that it can be decrypted by the human visual system if the correct key images are used. The technique was proposed by Moni Naor and Adi Shamir[6] in 1994. According to them Visual Cryptography is a method of encrypting a secret image into shares such that stacking a sufficient number of shares reveals the secret image. Shares are binary images usually presented in transparencies. Unlike conventional cryptographic methods, VC needs no complicated computation for recovering the secret image. The act of decryption is to simply stack shares and view the secret image that appears on the stacked shares. Visual Cryptographic technique is being used for secretly transfer of images in army, hand written documents, financial documents, text images, internet- voting etc. VC shares exist in their actual form during the transmission over network. However, directly third person cannot guess the secret information with any single share, but there is a possibility of retrieval if hackers are able to collect all the shares passing in sequence over the network. Thus to get rid of this problem, we need to enhance the security of shares. For the same purpose we have used Public Key Cryptography in addition to Visual Cryptography so that even if hackers are able to get all the shares but they cannot retrieve the original secret without the access of private key.

II. RELATED WORK

Various researches have been carried out in this area to increase the security & visual quality of the secret image. Some of them are as follows: Néelima Guntupalli et al [5] presented survey of various Visual Cryptographic Schemes and established the conceptual knowledge about Visual Cryptography. Yogesh Bani, Dr. B.Majhi, Ram S. Mangrulkar [13] proposed a novel approach for Visual Cryptography using Data Hiding by Conjugate Error Diffusion watermarking technique. Two shares have been generated and then embed into the cover image x with the help of watermarking. Secret and cover images have been revealed after overlapping shares. Cover image consume extra storage space. Intruder can attack on the shares to reveal the secret, which causes disturbance in the pixels of original image and the receiver will not get the actual secret. At the receiver end the cover image and secret both will be revealed, so the quality will be poor image. Debashish Jena,

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

Sanjay Kumar Jena [4] implemented Data Hiding using Conjugate Ordered Dithering (DHCOD) algorithm for generating the shares. A dithered halftone image generated by the cover image was the first share. For second share, some noise was added to the secret image and converted it to the binary image after that using share 1 and binary image they generated the second share. The secret image has been revealed with the simple AND operation of share 1 and share 2. Share generation process is made complicated by this method. B. Padhmavati, P. Normal Kumar, M. A. Dorai Rangaswamy [2] generated shares first by Visual Cryptography VC (2, 2) scheme. Then both shares were embedded into the cover images with the help of watermarking. For reveal of secret image, the extraction process was used to extract the shares from the embedded images. At last both shares were overlapped and revealed the secret image. Two cover images have been used to hide the shares which require extra memory space. M. Nakajima, Y. Yamaguchi [7] suggested Extended Visual Cryptography for natural images. Three input pictures have been taken; one is secret and other two for encryption. The encryption process is based upon determining the arrangements of transparent sub pixels on two images (used to conceal the existence of third secret image) according to the pixel transparencies, $t1$, $t2$ and tT. Where, tT is the transparency of target image. The secret picture is reconstructed by printing the two output images on transparencies and stacking them together. The problems with this technique are network overload due to two extra images and poor quality of revealed image. Wei-Qi-Yan, Duo Jin, Mohan S Kankanhalli [12] suggested a solution for superimposition of two shares. Some alignment marks are used in Walsh transform domain. It is always beneficial to use the scheme developed by this author, because in VC decryption stacking of two shares is mandatory and without exact alignment retrieval is not possible. Abhishek Parakh and Subhash Kak [1] suggested Recursive Hiding scheme for 2 out of 3 secret sharing. Secret bit is divided into 3 pieces p1, p2, p3.

For 0 p1=p2=p3 as 000,111, 222

For 1p1≠p2≠p3 as 021,102,120,210,201etc

Shares of smaller message are used to create shares of larger message. This scheme helps in decreasing the network load. Per pixel 9 bits expansion if the image size is multiple of 3, 16 bits expansion if image is multiple of 4 and so on this is not acceptable after a limit. Currently the efficiency of this system is 33% which will decrease as the size will not be exactly in multiple of 3. Vaibhav Choudhary et al [11] discussed an Improved Pixel Sieve Method for Visual Cryptography used an additional sieve to generate shares. In this scheme Secret is hidden properly using this scheme but efficiency of this scheme cannot be evaluated as decryption algorithm and the results of retrieval have not been shown in the paper. Ujjwal Chakraborty et al [10] proposed two schemes for (2, 2) and (2, 3) visual cryptographic encryption. The first scheme considers 4 pixels of input image at a time and generates 4 output pixels in each share. The second scheme considers 2 pixels (1 block) of input image at a time and generates 3 output pixels in each share. The dimension of revealed image is increased by 1.5 times in horizontal direction and remains same in vertical direction. Shyamalendu Kandar & Arnab Maiti [9] has proposed a technique of k-n secret sharing on color images. At the time of dividing an image into n number of shares, they have used random number generator. Minimum k numbers of shares are sufficient to reconstruct the image. If k numbers of shares are taken then the remaining shares are (n−k). In an image if certain position of a pixel is 1, then in (n−k) +1 number of shares in that position of that pixel there will be 1. In the remaining shares in that position of the pixel there will be 0. A random number generator is used to identify those (n−k) +1 number of shares. Secret is not properly hidden and it is easy to guess the contents in all three shares. If intruder is able to get the information about randomness, secret image can be retrieved. Chandramathi S, Ramesh Kumar R, Suresh R & Harish S [3] in 2010 concluded from the overview of all existing VC schemes that researchers should focus on good quality of reconstructed image & to increase security with minimum pixel expansion. P. S. Revenkar, Anisa Anjum and W. Z Gandhare [8] evaluated the performance of various Visual Cryptographic Schemes, which help in choice of best scheme according to the available bandwidth or color of secret image or level of security required. Following parameters have been used to evaluate the performance:

- No. of Secret images
- Pixel Expansion
- Image Format
- Type of shares generated

As we have observed that conventional cryptography is not used to protect the shares. In some cases cover images are used to carry the secret share which is an extra overload on network. This limitation forced us to use Public Key cryptography which provides shares with change in actual information.

III. METHODOLOGY OF THE PROPOSED SCHEME

The proposed scheme generates the encrypted image by applying pixel index reverse, zigzag and RSA algorithm of public key cryptography and then generates VC shares using visual cryptography so that the secret shares will be more secure and shares are protected from the malicious adversaries who may alter the bit sequences to create the fake shares. During the decryption phase, secret shares are extracted by staking the shares together & applied RSA decryption algorithm to reveal the secret image. As shown in Fig.1, complete scheme is divided into following five steps:

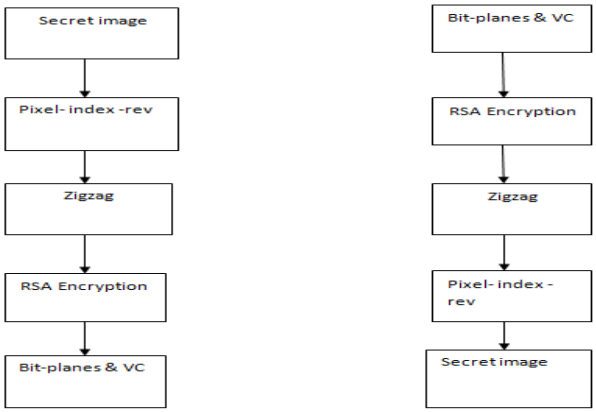


Figure 1: Methodology of the Proposed Scheme

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

Encryption:

1. **Reading the secret image:** In this step we are going to read the secret image.

2. Pixel index reverse: in this step the index of the secret image is reversed and rearranged the pixels of the secret image according to the new index values.

3. Zigzag: In this step the pixels of the secret image is arranged in zigzag pattern.

4. Encryption using RSA: in this step we will encrypt the image generated from the previous step. We have used RSA for encryption in this step. First we have generated the key for RSA and then performed the encryption.

5. Applying VC: In this phase Visual Cryptography Encryption is implemented. It consists of generation of shares from secret image using VC (2, 2) scheme. The secret image is first converted into a binary image then each pixel in the secret image is broken into 8 sub pixels, 4.pixels in each share by selecting the random pixel encoding scheme out of three given in Fig.2.

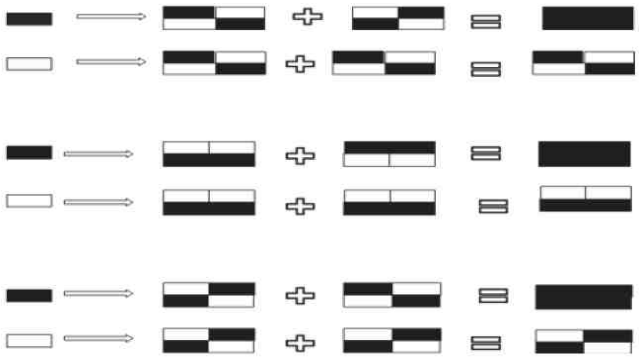


Figure 2: Pixel encoding schemes

Decryption:

1. Reading the VC shares: in this step the visual cryptographic shares are read.

2. Cryptographic decryption: In this phase Visual Cryptographic decryption is performed. We have decrypted the original secret image by applying the binary XOR operation on decrypted shares.

3. Decryption using RSA: in this step we apply RSA decryption algorithm to the image generated in the previous step.

4. Reverse Zigzag: in this step reverse zigzag pattern applied to the image generated in the previous step.

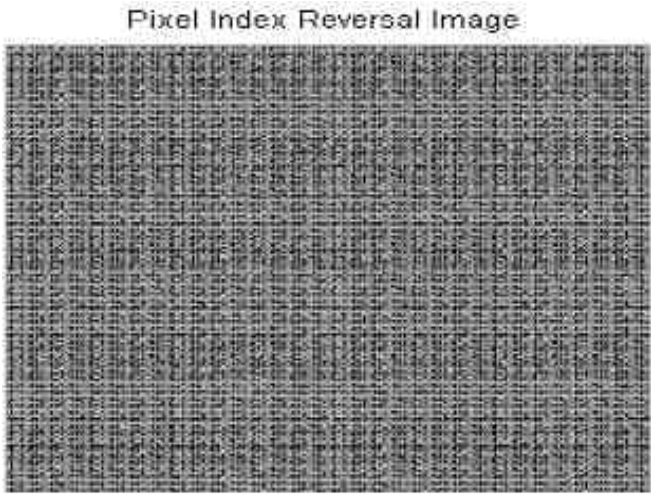
5. Reverse pixel index: This process takes place at the destination of the decryption process. Here the pixel index reverse applied to the image and we obtain the original image.

IV. EXPERIMENTAL RESULTS

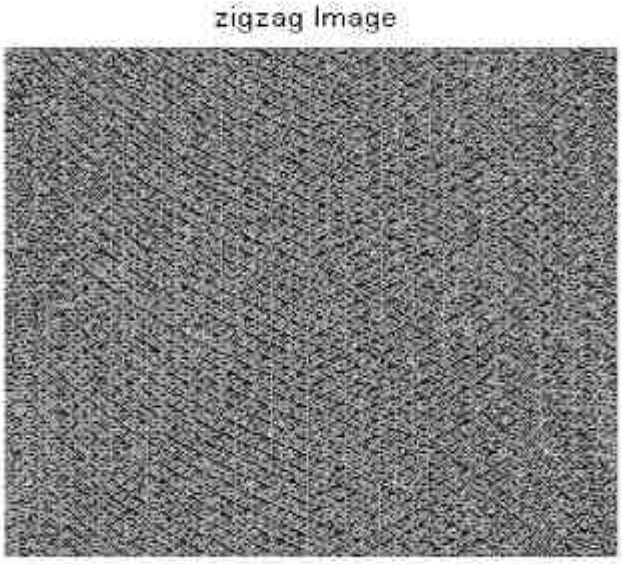
Proposed scheme has been implemented in MATLAB 7.14. To run this scheme minimum hardware configuration is required with no extra specifications. The experiments have been run in Windows 8 on a Sony VAIO laptop with Intel i3 2.4 GHz processor. To test the performance of this scheme number of experiments as been conducted with varying image sizes, types & keys but every time secret image is retrieved with good visual quality. The confidentiality of shares is also tested by super imposing the encrypted shares before reaching to the destination. Result is shown below. This experiment has been conducted taking secret image as shown step1, in step 2 the pixel index reverse is done .in step 3 the image pixels are arranged in zigzag pattern. The result of zigzag image in encrypted in step 3 using RSA algorithm. Step 4 shows the conversion of RSA encrypted image into bit planes. Step 5 shows the encrypted shares of visual cryptography and in step 6 X and Y shares are combined and 2 gray images are obtained.

1. Secret image

2. Pixel index reverse

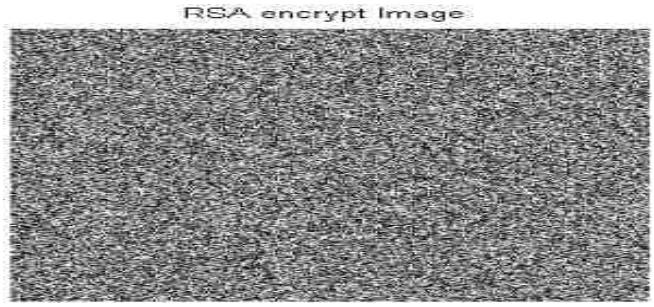


3. Zigzag

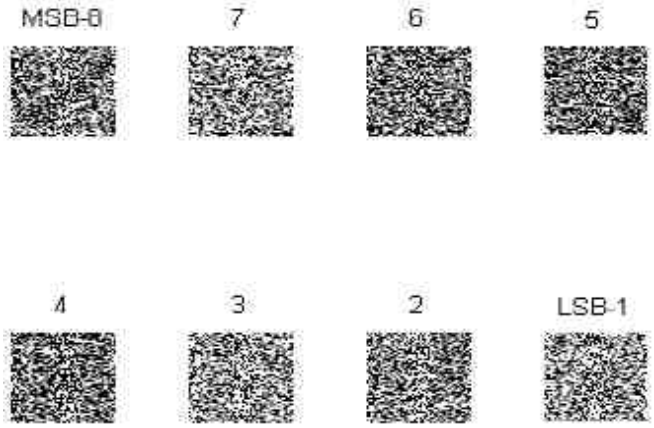


Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

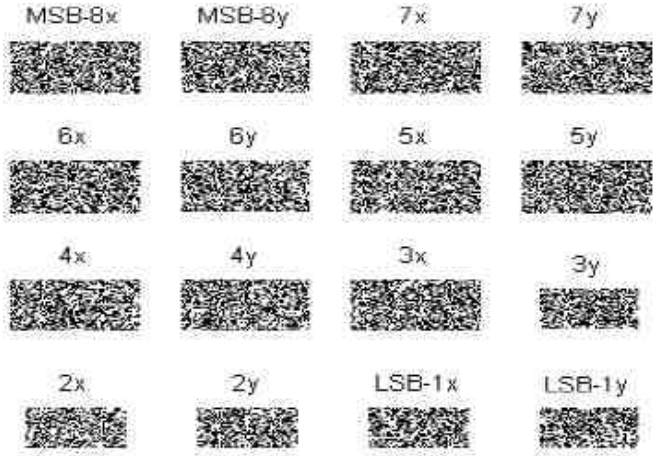
3. RSA Encryption



4. Bit planes

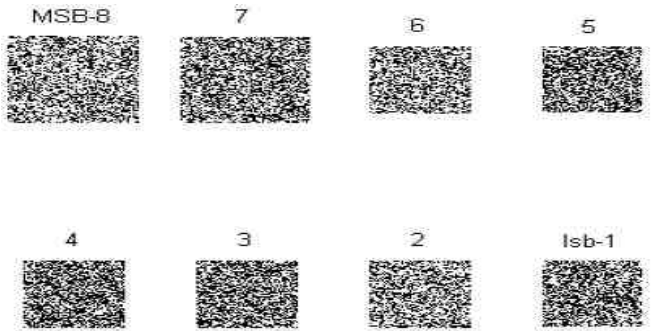


5. Visual cryptography

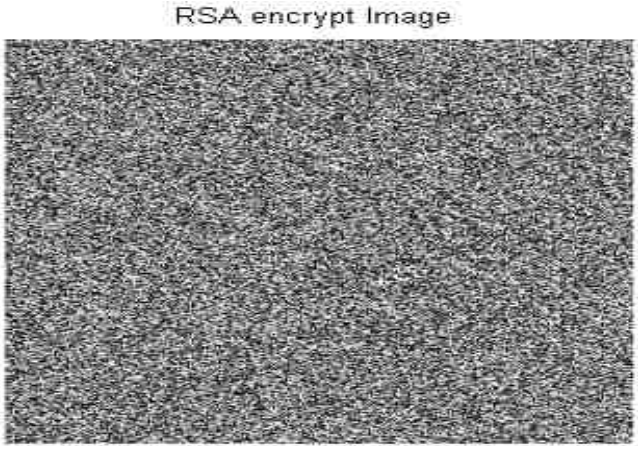


6. Encrypted gray image

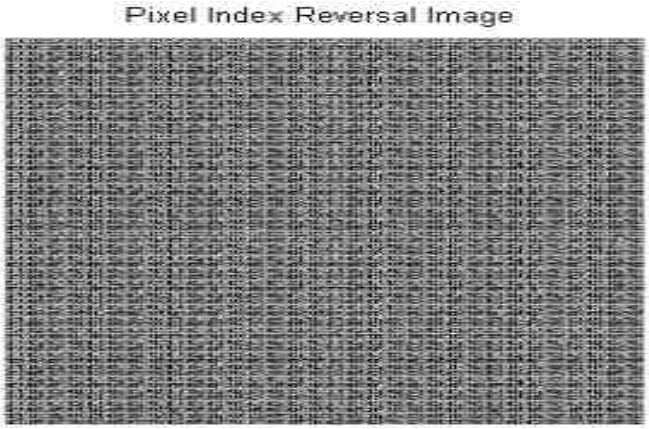
7. VC decryption



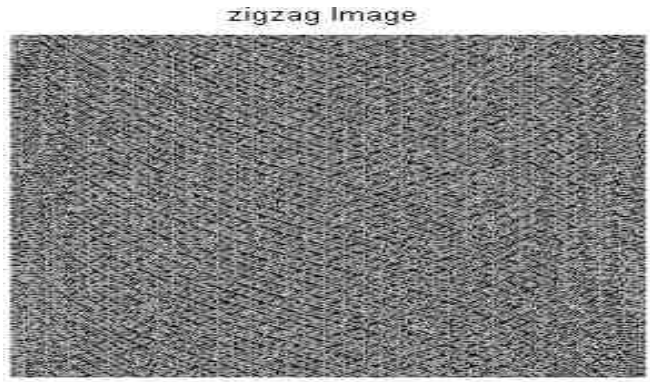
8. RSA decryption



9. Inverse zigzag



10. Index reverse



11. Decrypted secret image

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

Step 7 to step 11 shows the decryption process where in step 7 the reveres visual cryptography is applied and bit planes are obtained. These bit planes are combined and RSA decryption is applied and got RSA decrypted image in step 8 .in step 9 inverse zigzag is performed. Finally the inverse pixel index reverse is done in step10 and we get back the secret image in step 11.Performance of the scheme has been evaluated to test Whether retrieval of input images have been possible by any opponent having all the shares at the same time by stacking encrypted shares. The proposed scheme has been implemented on FPGA. The hardware has been designed for encryption/decryption of 16 pixels once and this process is continued till the last pixel of the image. Finally we obtain the encryption/decryption of entire image. The simulation results are shown in below figures.

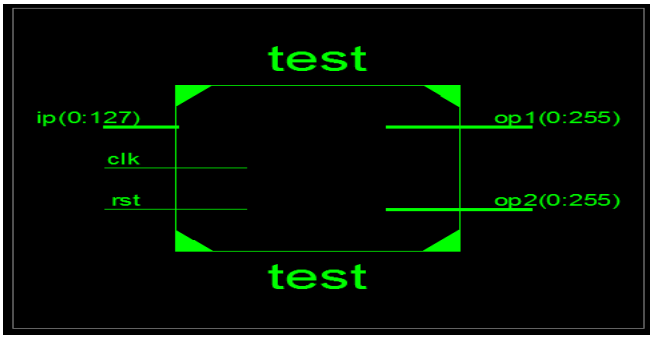


Figure 4.1: RTL schematic of encryption

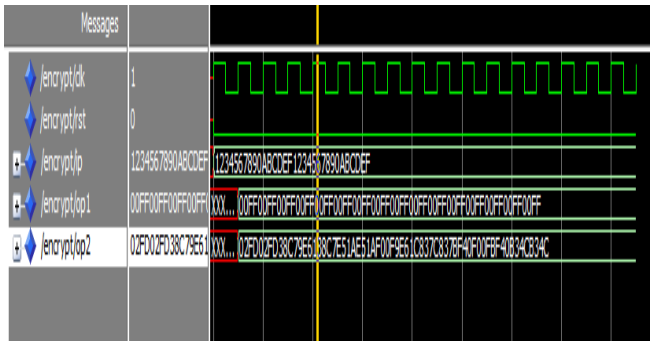


Figure 4.1: output waveform of encryption

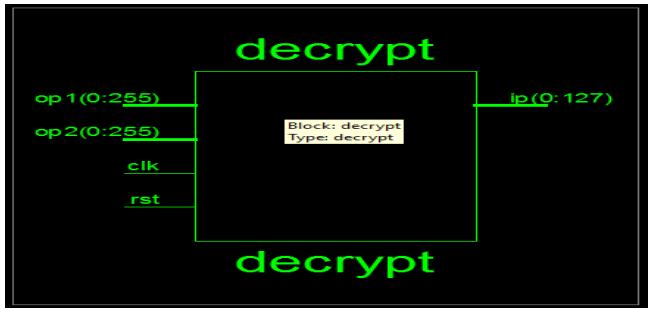


Figure 4.1: RTL schematic of decryption

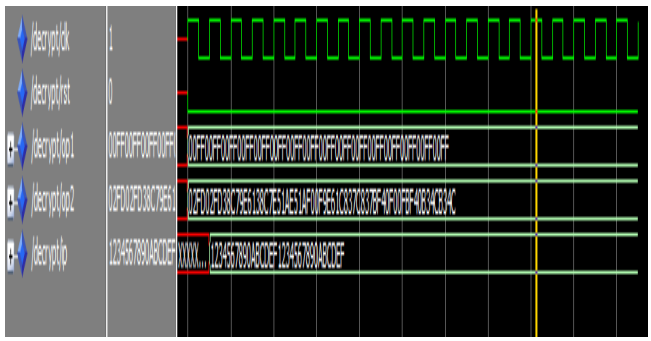


Figure 4.1: output waveform of decryption

V. CONCLUSION & FUTURE SCOPE

I have tested this scheme on different types of input images with change in size of the image and keys of RSA. But the entire time secret image is retrieved with good visual quality. The confidentiality of shares is also tested by super imposing the encrypted shares before reaching to the destination. In all the cases it has been observed that if any intruder will be successful to get the encrypted shares from network, he or she cannot retrieve the original secret image without availability of private key. It has been observed that there are many possible enhancements and extensions exist as the visual quality & size of revealed image. The major areas of future scope are:

- We can use color image in place of binary image and then generate the shares using Visual Cryptography.
- Compression of encrypted shares to reduce bandwidth requirement
- Size of image
- Variations in format of Input image

REFERENCES

[1] A. Parakhand S. kak"A Recursive Threshold Visual Cryptography Scheme" .Department of Computer Science, Oklahoma State University Stillwater,OK74078.

[2] B. Padhmavati, P. Nirmal Kumar, M. A. Dorai Rangaswamy"A Novel Scheme for Mutual Authentication and Cheating Prevention in Visual Cryptography Using Image Processing". Department of Computer Science &Engineering, Easwari Engineering College, Chennai, DOI: 02, ACS.2010.01.264, 2010 *ACEEE*.

[3] Chandramathi S, Ramesh Kumar R., Suresh R. and HarishS. "An overview of visual cryptography" *International Journal of Computational intelligenceTechniques*, ISSN: 0976–0466&E-ISSN: 0976–0474Volume 1, Issue 1, 2010, PP-32-37

[4] D. Jenaand S. Jena "A Novel Visual Cryptography Scheme".

[5] Néelima. Guntupallietal ,"An Introduction to Different Types of Visual Cryptography Schemes" ,*International Journal of Science and Advanced Technology* (ISSN2221-8386),Volume 1No7September 2011,PP198-205.

[6] M. Naorand A. Shamir "Visual Cryptography". Advances in Cryptology EUROCRYPT '94. Lecture Notesin Computer Science, (950):1–1, 1995.

[7] M. Nakajima and Y. Yamaguchi "Extended Visual Cryptography for Natural Images" .Department of Graphic and Computer Sciences, Graduate School of Arts and sciences, the University of Tokyo 153-8902, Japan.

[8] P.S.Revenkar, Anisa Anjum, W.Z.Gandhare "Survey of Visual Cryptographic Schemes". *International Journal of Security and Its Applications*Vol.4, No.2, April, 2010.

[9] Shyamalendu Kandar & Arnab Maiti **"**K-Secret Sharing Visual Cryptography Scheme for Color Image Using Random Number". *International Journal of Engineering Science and Technology (IJEST)*, ISSN0975-5462, Vol.3 No.3Mar201, PP1851-1857

[10] Ujjwal Chakrabortyet al, "Design and Implementation of a (2,2)and a(2,3) Visual Cryptographic Scheme" *International Conference [ACCTA-2010]*,Vol.1Issue2,3,4, PP128-134

[11] Vaibhav Choudhary "An Improved Pixel Sieve Method for Visual Cryptography" *International Journal of Computer Applications*,(0975–8887)Volume12–No.9,January2011.

[12] Wei-QiYan, DuoJin, Mohan S Kankanhalli "Visual Cryptography for print and scan applications "School of Computing ,National University of Singapore,Singapore117543

[13] Y. Bani, Dr. B. Majhiand R.S. Mangrulkar,2008. A Novel Approach for Visual Cryptography Using a Watermarking Technique. In *Proceedings of 2nd National Conference ,India Com2008*.

[14] Behrouz A. Forouzon, "Cryptography & Network security"4th Edition.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.