# Implementation of Encrypted Visual Cryptographic Shares using RSA algorithm on FPGA

**Manojkumar.G.L**
Department of Electronics& Communication Engineering
PES College of Engineering,
Mandya, Karnataka

**Subramanyam.M**
Associate prof , Department of Electronics &Communication engineering
PES College of Engineering,
Mandya, Karnataka.

***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 w ho 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.**

***Keywords---Visual Cryptography; Encryption; Information Security;VCshares***

## I. INTRODUCTION

,Q WRGD\¶V LQIRUPDWLRQ DJH_ LQIRUPDWLRQ VKDULQJ WUDQVIHU 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.

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, 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. Nirmal 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, *t*1, *t*2 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
)RU _S_ • S_ • S_ DV _____HWF

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 (níN__ ,Q DQ LPDJH LI FHUWDLQ SRVLWLRQ RI D SL[HO LV __ WKHQ LQ _QíN_ __ 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 thoVH _QíN_ __ 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 VC shares using basic Visual Cryptography model and then encrypt both shares using RSA algorithm of Public Key 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 RSA decryption algorithm & stacked to reveal the secret image. As shown in Fig. 3.1, complete scheme is divided into following four phases:

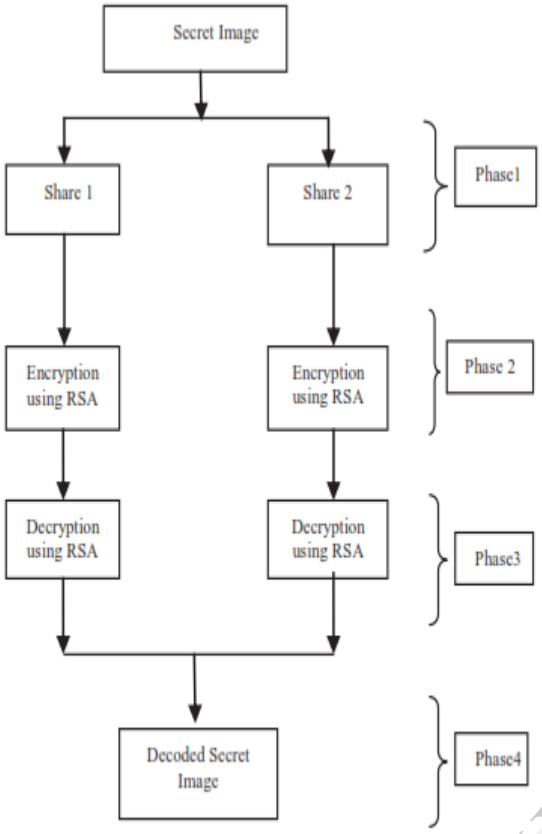



Fig.3.1 Methodology of the Proposed Scheme

A. *PHASE-1 Generating shares of secret image:* 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.3.2.

B. *PHASE-2 Encrypting the generated Shares:* This is the second phase of our approach which will encrypt shares generated from the first phase. We have used RSA for encryption in this step. First we have generated the key for RSA and then performed the encryption. Results of this phase are encrypted shares.

C. *PHASE-3 Decrypting the Shares using RSA:* This process takes place at the destination of the document/image/text. We again convert the encrypted shares in their actual form using RSA decryption algorithm, which were encrypted at the sender end.

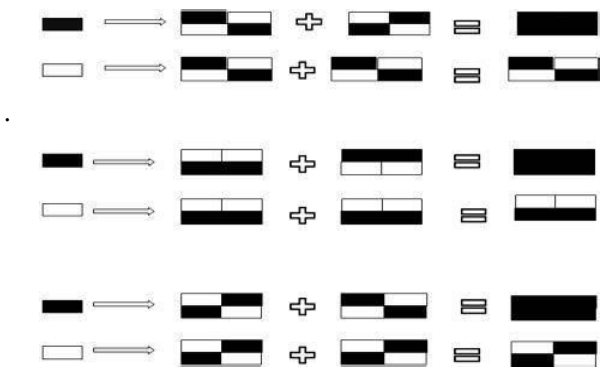


Fig. 3.2. Pixel encoding schemes

D. *PHASE-4 Visual Cryptographic decryption:* In this phase Visual Cryptographic decryption is performed. We have decrypted the original secret image by applying the binary XOR operation on both decrypted shares.

The algorithms for conversion of image into binary and share generation are given below:

```
Image-conversion
Input:          .jpg image/.bmp image
Output:         BIN_IMG, R_size, C_size
IMG=read ()
BIN_IMG=Convert_to_binary (IMG)
[R_size  C_size]=Cal_size (BIN_IMG)
```

Algorithm 3.1 Image Conversion

```
Share_generation
Input:          BIN_IMG, R_size, C_size
Output:         SHARE1
                SHARE2
For i=1 TO R_size
Do
        For j=1 TO C_size
        Do
        Pix_enc_scheme=Rand_select()
SHARE1=Pix_enc_scheme(BIN_IMG(i,j))
SHARE 2=Pix_enc_scheme(BIN_IMG(I,j))
        Done
Done
```

Algorithm 3.2 Share Generation

## IV. EXPERIMENTAL RESULTS

Proposed scheme has been implemented in MATLAB 7.5. To run this scheme minimum hardware configuration is required with no extra specifications. The experiments have been run in Windows 7 on a Sony VAIO laptop with Intel i5 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. Results of some experiments are shown in Fig.4.1, Fig.4.2 & Fig.4.3.

These experiments have been conducted taking secret LPDJHV RI GLIIHUHQW VL]HV DV DQ LQSXW VKRZQ E\ Fig.4___)LJ____ & )LJ_____ µ%¶ & µ&¶ VKRZ VKDUH_ & VKDUH

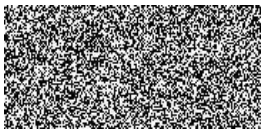
the secret image generated by the Visual Cryptographic encryption phase µ'¶ & µ(¶ VKRZ WKH HQFU\SWHG VKDUH_ & encrypted share2. These are the results of second phase, in which the Visual Cryptographic shares have been encrypted XVLQJ HQFU\SWLRQ DOJRULWKP_ µ*¶ & µ+¶ VKRZ WKH GHFU\SWHG share1 & decrypted share2, the results of decryption phase XVLQJ 56$_ µ,¶ VKRZV WKH RULJLQDO VHFUHW LPDJH UHYHDOHG E\ overlapping the decrypted share1 and decrypted share2. The Visual Cryptographic decryption is used to retrieve this secret image.



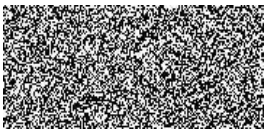
**A. Binary Input Image1**

**B. Image1_share1**

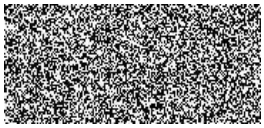
**C.Image1_share2**



**D. Image1_Encrypted share2**



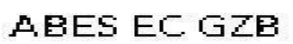
**E. Image1_Encrypted share2**



**E.Revealed Image from Encrypted shares**

**G.Image1_Decryptedshare1**

**H.Image1_Decryptedshare2**

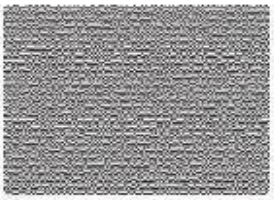


**I.RevealedImage1fromdecryptedshares**

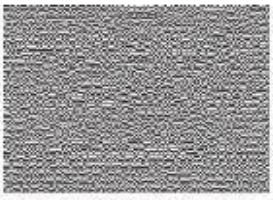
Fig. 4.1 Experiment-1

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 HQFU\SWHG VKDUHV_ ,Q )LJ_____ )LJ____ & )LJ____ µ) VKows the result of stacking encrypted shares which prove that opponent cannot retrieve secret image without having secret key. Table I shows that system is enough efficient with the varying size of input and random selection of key.

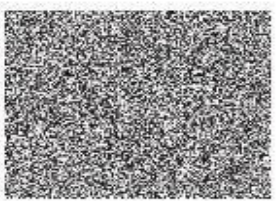
**A. Binary Input Image2**



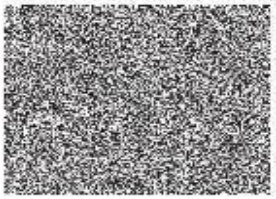
**B. Image2_share1**



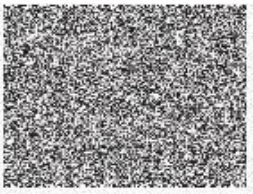
**C. Image2_share2**



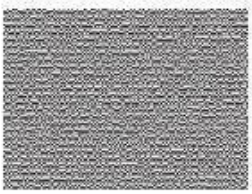
**D. Image2_Encrypted share2**



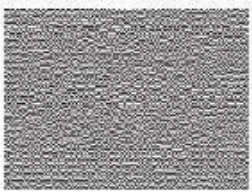
**E. Image2_Encrypted share2**



**F. Revealed Image from Encrypted shares**



**G. Image2_Decrypted share1**

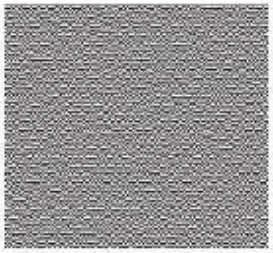


**H. Image2_Decrypted share2**

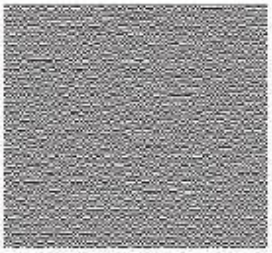
**I. Revealed Image2 from Decrypted shares**

Fig. 4.2 Experiment-2

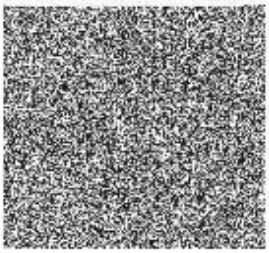
A. Binary Input Image3



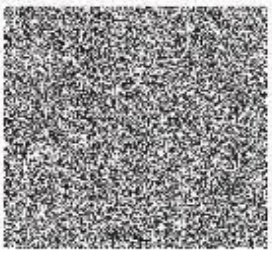
B. Image3_share1



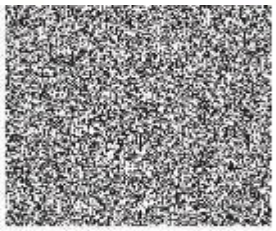
C. Image3_share2



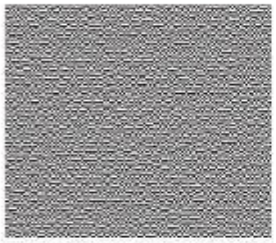
D. Image3_Encrypted share2



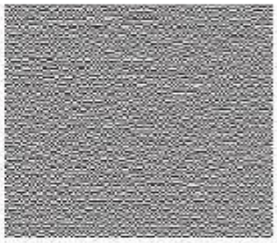
E. Image3_Encrypted share2



F. Revealed Image from Encrypted shares



G. Image3_Decrypted share1



H. Image3_Decrypted share2

Fig. 4.3 Experiment-3

Table I. System Performance

| Input Image (size) In Pixels | Public Key (e, n) | Private Key (d, n) | Retrieval after stacking encrypted shares | Retrieval after stacking decrypted shares |
|---|---|---|---|---|
| (38X90) | (25,163202) | (77929, 163201) | Not Retrieved | Retrieved |
| (80X96) | (53,511493) | (404189, 511493) | Not Retrieved | Retrieved |
| (80X96) | (13, 92341) | (56229, 92341) | Not Retrieved | Retrieved |

## V. CONCLUSION & FUTURE SCOPE

We 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. We have implemented the encrypted shares on FPGA successfully.

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
  - More sophisticated public key encryption to reduce key size
  - Size of image
  - Variations in format of Input image

## REFERENCES

[1] A.ParakhandS.kak³A Recursive Threshold Visual Cryptography Scheme´ .Department of Computer Science,Oklahoma State University Stillwater,OK74078.

[2] B.Padhmavati,P.NirmalKumar,M.A.DoraiRangaswamy³A Novel Scheme fo 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] ChandramathiS., Ramesh Kumar R., Suresh R. and HarishS. ³An 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 ³A Novel Visual Cryptography Scheme´.

[5] Néelima.Guntupallietal ,³An Introduction to Different Types of Visual Cryptography SchemeV´ ,*International Journal of Science and Advanced Technology* (ISSN2221-8386),Volume 1No7September 2011,PP198-205.

[6]M.NaorandA.Shamir ³VisualCryptography´. Advances in Cryptology EUROCRYPT ¶94. Lecture Notesin Computer Science, (950):1±1, 1995.

[7]M.Nakajima and Y.Yamaguchi ³(xtended Visual Cryptography for Natural ImageV´ .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 ³6urvey of Visual Cryptographic SchemeV´_ *International Journal of Security and Its Applications*Vol.4, No.2,April ,2010.

[9]ShyamalenduKandar & ArnabMaiti **"**K-NSecret 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] UjjwalChakrabortyet al, ³Design 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 ³An 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 ³Visual Cryptography for print and scan applications ³6chool of Computing ,National University of Singapore,Singapore117543

[13] Y.Bani, Dr. B. MajhiandR.S. Mangrulkar,2008. ANovel Approach for Visual Cryptography Using a Watermarking Technique.In *Proceedings of 2nd National Conference,IndiaCom2008*.

[14]BehrouzA. Forouzon, ³Cryptography & Network security´4th Edition.