Enhanced Security Architecture for Visual Cryptography Based on Image Secret Sharing

Manas Abhilash Gundapuneni
Department of Computer Science and Engineering
Motilal Nehru National Institute of Technology Allahabad
Prayagraj, India
gundapuneni.manas@ieee.org

Anzum Bano
Department of Computer Science and Engineering
Motilal Nehru National Institute of Technology Allahabad
Prayagraj, India
anzumsalim0786@gmail.com

Navjot Singh
Department of Computer Science and Engineering
Motilal Nehru National Institute of Technology Allahabad
Prayagraj, India
navjot@mnnit.ac.in

***Abstract*—This paper provides an approach to a new encryption architecture using double layer encryption standards for the existing secret sharing methodology. The image encryption standard in this scheme deals with both gray scale and color images and provides the experimental results. The paper deals with the transmission of multimedia such as images over insecure and secure networks, secret sharing helps to mask the image from the attacker by breaking it down to shares which are not at all related in the sense of content to the original image and provide the security of only reconstructing the original image when the client has all the shares.**

***Index Terms*—Visual Cryptography, Secret Sharing, Cellular Automata**

I. Introduction

In the wake of rapid digitization in various technological fields, secure data transmission over networks has become an essential area of research. After recent advancement of the hand-held devices and image capturing systems, images are being used in various processes such as customer verification, identification or authentication which has increased the amount of multimedia data transmitted over the networks. The encryption standards being used for encrypting multimedia remains the same, as the modern cryptography standard used in the sequential or block/chunk data processing. The requirement for a cryptography standard in multimedia transmission is of demand and not drafted into industry utilization. The computation complexity associated with AES/RSA encryption standards is too intensive and has increased the load on devices due to increased video streaming , video calling and image sharing taking place on the social media or the internet. Use of the traditional encryption takes a lot of time to encrypt each frame of image data in a format agnostic to the retrieving media.

Department of Science and Technology, Government of India

978-1-7281-9656-5/20/$31.00 ©2020 IEEE

Visual Cryptography is the paradigm shift started for creating an encryption standard exclusively for multimedia data. This has led to development of alternate Cryptography techniques which could encrypt the data efficiently and decrypt effortlessly.

Secret sharing scheme by [5] has given the foundations of the mathematical research towards the multi-cryptography standard. The secret sharing scheme initially described for numerical data had been extended to working with the images and multimedia by [1] as Visual Cryptography in 1994. Visual Cryptography deals with the multimedia information to be encrypted by the means of which image cannot be decoded by visual information systems. In the following years [9] developed a scheme for colored images. The drawbacks of these schemes were mainly the meaningless shares being used for encryption which make the quality of the recovered secret implausible than the original secret.

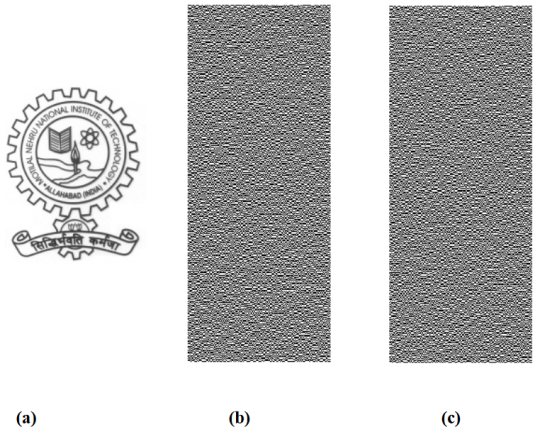
Later [2] had introduced in the year 2000 a lossless scheme which used a Color Index Table(CIT) and was aberrant from the stacking mechanism of transparencies used and didn't require it, which made it easier to use in the real time applications. But as the colors present in the secret image increased the CIT became larger, pixel expansion factor became significant which increased the loss of resolution in contrast to the scheme. Visual Cryptography taken independently is not sufficient to conform to the secure and safe transmission of the multimedia over the internet and would require an additional layer of security.

Visual Cryptography can be classified into

1.Random Grid based VCS (RGVCS) schemes

2.Polynomial based Secret Image Sharing (Polynomial based SIS) schemes

Random Grid Based VCS use the concept of randomness and cannot provide 100% accuracy, whereas the Polynomial Based VCS construct a polynomial based on the pixels of the secret image.



(a) (b) (c)

Fig. 1. Naor and Shamir (2,2) VCS (a) Secret Image (b)Share 1 (c) Share 2

II. Motivation

The motivation for proposed architecture and technology is, after studying various observations of research in the field it had been identified that even though multimedia is encrypted in the traditional modern cryptography standards , the Electronic Code Book type of encryption standards reveal the sleuth of the image , meaning the outlook of the image can be reconstructed by the attackers in the network as shown in Fig 3. The importance of data has been of prime importance for securing and transmitting it and data transmission has become critical. It is essential to have a scheme which transfers the data from one point to another without giving any third party a chance to decode it. A double layered architecture is required to transfer data securely and provide a enhanced security for the primary mode of encryption based on the secret sharing principle.

III. Related Work

A. Naor and Shamir (2,2) Visual Cryptographic Scheme

A *k* out of *k* visual cryptography scheme is used in this method.In *(k,k)* scheme the master image or the master share is transformed into *k* shares. Each and every share in *k* shares is required for the retrieval of the master share [1]. If any shares less than *k* are used for reconstruction of the master share the reconstruction fails and does not reveal the secret or master share. A *(2,2)* scheme is constructed by Noar and Shamir , where a secret share is divided into two shares, here the two shares are made by separating sub pixels of the original image into two transparencies. The two shares generated can be termed as a cipher text share and a secret share or key share. Both these shares have no similarity or resemblance to the original secret image. The results of this scheme are shown in Fig. 1.

The scheme generates random shares and does not allow attackers to reconstruct the secret. The performance of this scheme is *O(1)* for encoding and decoding. But this scheme is prone to loss of contrast upon reconstruction, the recovery is not complete and undergoes pixel expansion.

B. Thein Lin Polynomial based (4,6) Threshold Secret Sharing

A *n* out of *k* visual cryptography scheme is used in this method. In *(n,k)* scheme the master share or the secret image is transformed into *k* shares. Out of *k* shares generated the condition for reconstruction requires at least *n* shares out of the *k* shares. This implies that if we have *(2,5)* secret sharing scheme in use, then at least 2 images out the 5 images generated are needed for reconstruction of the original image without any loss. Any amount of images less than the *n* images fail to reconstruct the image. A polynomial of degree *k-1* is generated using the *k* gray level pixel intensities as the *k* coefficients in the Thein Lin scheme [10].The major difference between the scheme we propose and this scheme is that the polynomial generation and execution of the scheme for reconstruction is complicated and compute intensive. we define the polynomial as

$$f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^{n-1} \quad mod \quad 251 \quad (1)$$

The scheme is an extension of Shamir's VCS that includes Polynomial based techniques, there is a 100% Image Recovery at Decrypting end (Lossless). But this scheme is only applicable to gray scale images, cannot be extended to multiple images and the scheme is highly encryption and decryption compute intensive which is not practical in general usage computational devices.

IV. Proposed Work

In this paper, authors propose an *Enhanced Security Architecture for Visual Cryptography Based on Image Secret Sharing* mechanism which aims to overcome the disadvantages of the existing work. This scheme is generalized i.e the shares generated can be flexible for change. A multi-secret sharing scheme gives the choice of share dynamics. A *(k,k) where k belongs to* $2 \leq k \leq n$ share scheme is used where the secret sharing is based upon on algorithm with no reconstruction complexity using logical operators. The proposed system is improved over the existing mechanisms which fail to address the color images having red, blue, green and alpha transparencies and are based on random binary assignment for the shares based upon the secret. A enhanced architecture is outlined with two layers of security for images to have a fail safe secret sharing scheme and a recoverable share generation. The proposed work is novel, there has been no work particular to creating a double layer encryption standard using visual cryptography and enhancing it with cellular automata encryption, this proposed work provides new results on it's performance. Recent works in this area have been concerned with creating more schemes of encryption which make them weak if all the shares are captured and the scheme applied is known to the attacker.

A. Cellular Automata based Encryption Layer 1

The first part contains the standard encryption, but uses a one dimensional cellular automata image encryption system

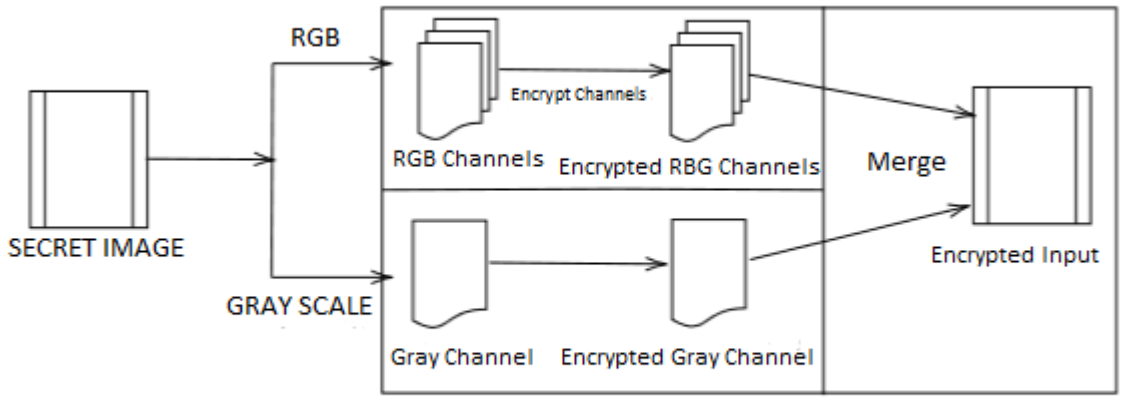


Fig. 2. Layer 1 Cellular Automata based Encryption

for scrambling the secret image as shown in Fig. 2. Cellular automata systems provide all the essential cryptographic properties and hardware support can be used. Cellular automata based systems provide improved system performance in comparison to traditional methods based on computational techniques [8]. Hence, this technique provides most favourable encryption systems. Image encryption can be done by reordering the pixels or transforming the pixel values or considering both. The Cellular automata encryption can be used in all the cases. Using cellular automata based encryption we also use the hardware support making it faster. Cellular automata encryption consists of large number of rule sets which are applied on individual pixels and offer a vast domain for the attacker to crack the encryption which makes it impossible for the attacker to check all the rule sets. This is a symmetric key encryption system which uses same set of keys for encryption or decryption.

CA systems are dynamic with discrete space and time. They are also abstract. A hybrid cellular automata process is used in this layer of security and the value obtained is substituted in the gray scale. [7]

The CA system is applied on the images by considering a image in the form of regular lattice composed of finite cells. The cells are finite and changed using local update rule set. The local update rule set works on the images pixel values by changing their state based on their current state and its neighbors pixel states.A cellular automata rule set consists of a matrix S denoting cell's state, T for local update rule and N set of neighbors. [7]

Rule set used for encryption of the 2D image are *R90*, *R10* and *R120*, this set can be expanded to custom declared rules of state changes also such as *R30* which is more complex and provides random generations in further iterations. The proposed algorithm for the layer 1 of the architecture

Rule	**111**	**110**	**101**	**100**	**011**	**010**	**001**	**000**
R30	0	0	0	1	1	1	1	0
R90	0	1	0	1	1	0	1	0
R120	0	1	1	1	1	0	0	0

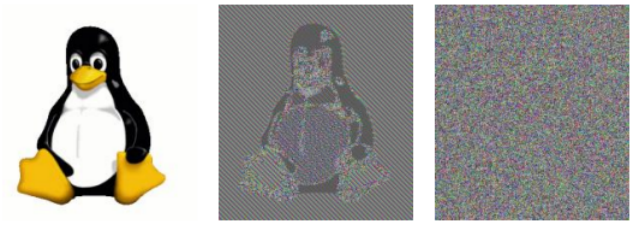
TABLE I: NEXT STATE TRANSITION OF RULE SET

1) ***Encryption Algorithm****:*

1: Input image and identify the color scheme format.
2: If RGB Image present separate each color channel.
3: Single Channel/Three Channels to 2D Matrix M.
4: Execute the key function on M.
5: Each kernel of M is transformed depending on the odd or even property of the pixel intensity by Key function depending and saved in the temporary file
6: Transformed kernel is fetched from buffer and converted into matrix.
7: The Cipher Matrix is now converted and stored as an Image.

2) ***Key Function****:*

1: Input kernel is split into 8 blocks.
2: Each block undergoes unique cellular automata transformation.
3: On Even Value Rule30 and Rule90 are applied alternatively.
4: On Odd Value Rule90 is performed.
5: Until initial input is repeated the rules are followed through.
6: Half of the cycle is calculated when recursion stage occurs as $hc = n/2$.
7: Decimal value is taken from the output of the array after conversion and stored in the input block.
8: All the above steps are looped until all values are processed.



(a) Original Linux Tux image (b) Encrypted Tux Image using ECB (c) Secret Sharing based Tux Image Encryption

Fig. 3. Depiction of Need for Secret Sharing

*3) **Decryption Algorithm**:*

1: Scrambled/Encrypted input image is divided into channels.
2: The Key Function is executed on each channel matrix.
3: Each kernel value is transformed from the odd/even value applied during the encryption saved in temporary file.
4: The Transformed kernels are stored in a new Matrix
5: The Matrix is converted back into an Image.

B. Generalized Multi transparency Image Multi-secret Sharing Scheme Layer 2

A Boolean operated highly secure secret sharing scheme has been designed for the usage of multi secret sharing. The need for this type of sharing arises directly from the vulnerabilities faced by the modern cryptography based encryption. Upon studying various works on how images have a high amount of correlation between pixels on the basis of context of the images it has been conceived that images are prone to human visual system decoding, as depicted by our study in Fig 3.

The Shadow image construction procedure or the share construction from the input and the output secret re construction from the shares is given in the format of definitions and pseudo code.

A Boolean XOR based operation has been employed to create shares, the shares created are meaningless shares as random shares are less susceptible to human visual system crypt analysis and offer more security than meaningful shares [4] [6]. The Secret after entering the system is termed as the Master Share and is used to modify based on the shares being generated randomly in their respective transparencies. A *(n,n)* secret sharing scheme is used in contrast to the *(k.n)* scheme present in major works, as the later scheme increases algorithm complexity by ways of need to generate redundant shares and wastes network bandwidth when incorporated. The proposed system is shown in Fig 4.

Input: A Image of format PNG, JPEG or TIFF, where the said image can be having RGBA Transparencies or a Gray Scale Transparency, an integer *N*, where *N* conforms to $N \geq 2$.

Output: *N* meaningless shares of PNG format in the same dimensions as the secret image out of which one is the master share indistinguishable.

Construction: The secret share given in the input , is converted into it's transparencies in the form of arrays of pixels namely numpy arrays, which then undergo the Cellular Automaton Encryption at each transparency level and are merged back together. The encryption here is carried out based on rules to be can selected and order can be changed (R30, R90, R120).

Random arrays of required transparencies are generated, operated on by the Boolean operator with the master share and the newly generated share. The operations can be quantified by the following equation

MasterShare = $Share_i \oplus MasterShare$
where $i \longrightarrow 0 \ \ to \ \ N$
where $share_i \ \ is \ \ generated \ \ by$
$rand_x(0, 254) * NumberofTransparencies$
where $x \longrightarrow 0 \ \ to \ \ height * width$

Revealing: The system takes as input a secret key file, *N* share and an integer *n*. The shares are then operated on by the Boolean operator for reconstructing the original secret image given as input to the system. A standard *uint8* representation is used throughout the system for the inter portability across construction and re-construction.

V. Experiments and Results

We shall present the experimental results of the proposed *(n,n)* secret image sharing scheme. A (4,4) secret sharing experiment is selected to demonstrate the performance of the proposed system. The test images 'Lena'(Color and Gray scale) are used as a secret image(input) for evaluating the systems resilience and robustness.

The results of the proposed enhanced security architecture is experimented on Lenna Gray Scale image and reported in Fig 5. The Fig 5.a is the input secret image given as input to the layer 1 cellular automata , which encrypts the input using symmetric encryption, as the image is gray scale , single channel is returned as an encrypted image Fig 5.b.

This encrypted image from layer 1 of enhanced architecture is given as input to the logical operator based secret sharing algorithm, a (4,4) scheme is chosen for encryption and 4 shares are given as output. All the shares are meaningless and offer an 2 layer security for the input image. Fig 6.g depicts the image reconstructed from the shares transmitted over the network.

The Fig 6.a shows Lenna Color image which is given as input to the layer 1, the Blue, Green and Red channels are split and individual channel is operated on by the layer1, after as show in Fig 6.b, Fig 6.c and Fig 6.d. The 3 encrypted channels are merged into a BGR color scheme as shown in Fig 7.a. The Encrypted Image from Layer 1 is given as input to the layer2 which generated the 4 shares as (4,4) scheme is used for experiment. The Image recovered after reconstruction can be see in Fig 7.f.

VI. Result Analysis and Practical Application

The resultant images after reconstruction can be evaluated by using the Peak signal-to-noise ratio, which is the signal to noise ratio, denoted by PSNR. It is the ratio between the maximum possible power of the signal to that of the corrupting

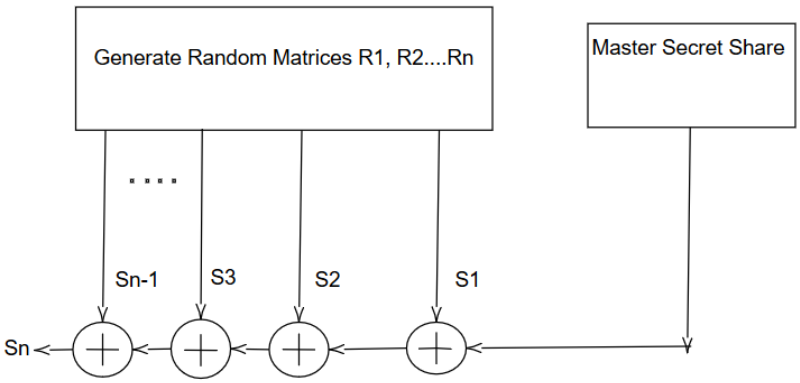


Fig. 4. Proposed Secret Sharing Share Generation

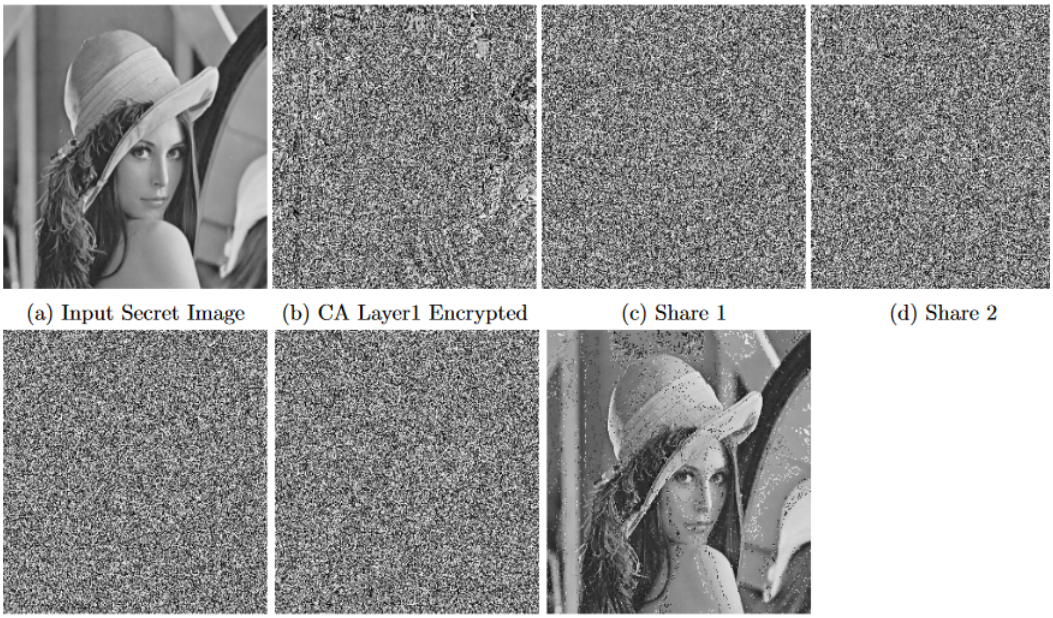


Fig. 5. Results of proposed architecture on Lenna Gray scale Image

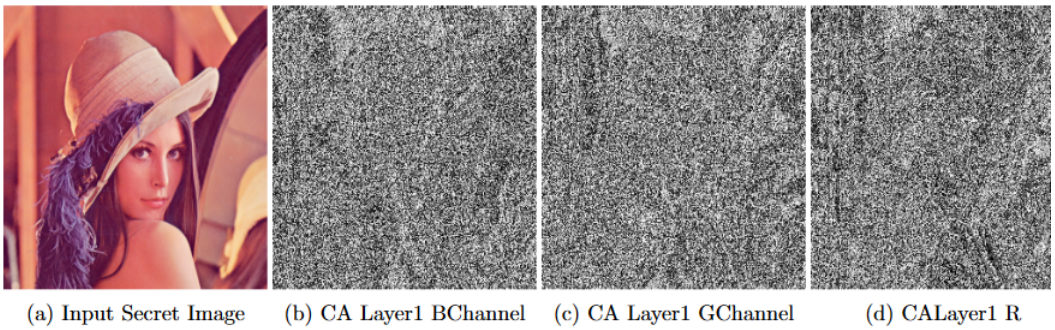
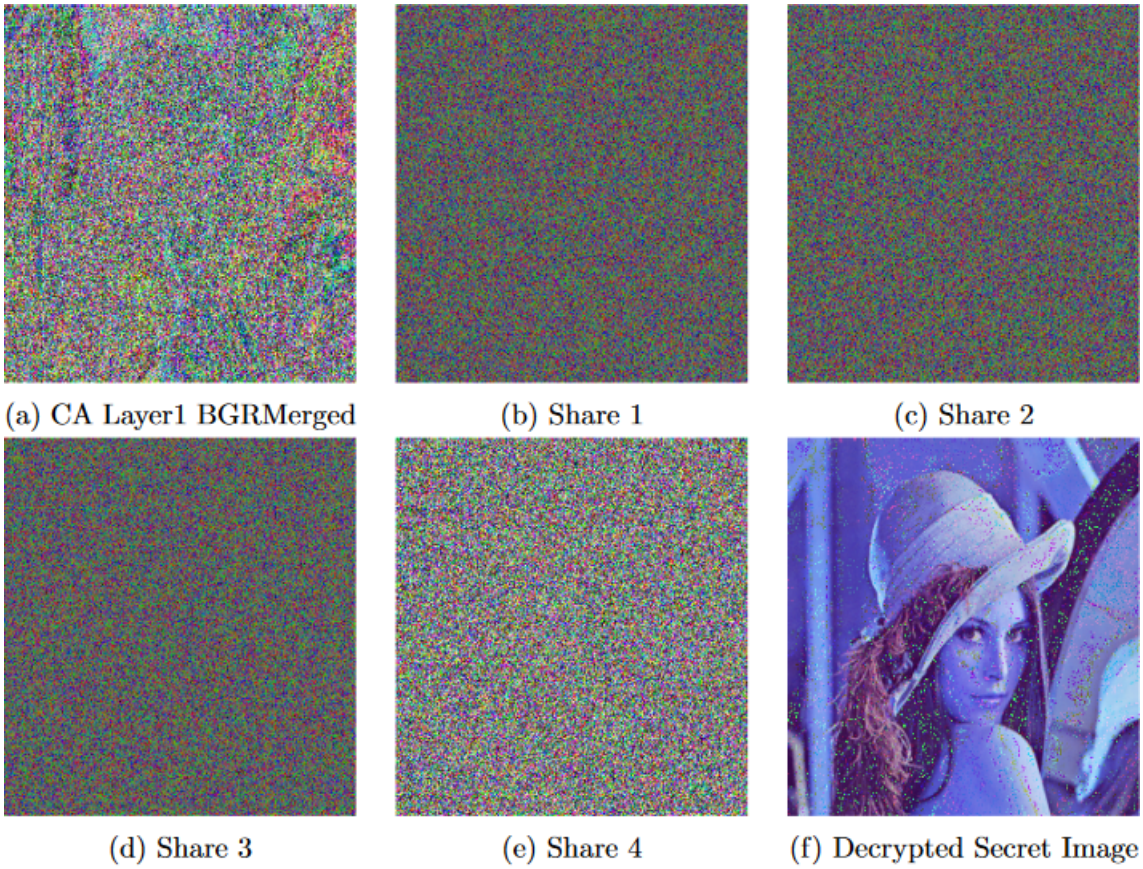


Fig. 6. Results of proposed architecture on Lenna Gray scale Image



(a) CA Layer1 BGRMerged (b) Share 1 (c) Share 2

(d) Share 3 (e) Share 4 (f) Decrypted Secret Image

Fig. 7. Results of proposed architecture on Lenna Gray scale Image

noise. PSNR is mainly used in the evaluation of the quality of reconstruction of lossy compression techniques. PSNR is usually measured in terms of logarithmic decibel scale, due to very wide dynamic range. The original image is considered here as the signal and the noise is taken from the reconstructed image due to errors. The quality of the image reconstructed even though high in terms of PSNR can not be compared to the images reconstructed with lower PSNR as they are more closer to the original image in terms of human perceptibly. [6]

The practical application of the proposed work are of significance in the health care industry, majority of the diagnostic centres have moved to electronic methods for providing reports, X-Rays or MRI. For transmission of such data, our work provides an edge of security as also discussed in [4]. The basic security architecture is not explicitly standardized in the industry but relies on the encryption provided by the network protocol standards to the higher layer applications sending data, this paper assumes the basic security architecture of being constituted of only a single layer of encryption in the field of visual cryptography or modern cryptography and there is no additional layer of security in place for securing the images explicitly. Even in [4] which uses XOR based scheme for store and forward tele-medicine [4], a single layer of encryption can be prone to attack when all the shares have been captured by a single entity and different approaches are tried to crack the image, using XOR to crack it might be an anticipation by the attacker, in view of such possibility our paper proposed an enhanced security architecture, where even though all the shares are captured and the scheme used in the visual cryptography is cracked and the image is reconstructed, the attacker can't crack the additional layer of cellular automata based encryption in place.

Particularly in the data centre's, the data is encrypted but the keys of the encrypted data are also stored at some place in the same data center and need to be secured, strength of the encryption technology can be undermined if the keys are exposed. Using our proposed scheme the keys can be embedded in the images and made into shares which can be stored at various data centre's, it is highly unlikely that all the data centre's will be compromised and even if they are the double layer encryption helps to secure the keys.

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (I(i,j) - K(i,j))^2 \tag{2}$$

Where MSE is mean square value, PSNR is defined as

$$PSNR = 10log_{10} \frac{R^2}{MSE} \tag{3}$$

Even though the PSNR value of the reconstructed image in case of the gray scale is low, the image is still suitable for

Experiment	PSNR
Lenna Gray Scale Image(jpg)	35.87
Lenna Color Image(jpg)	20.19

TABLE II: PSNR of proposed scheme

human perception with respect to the original secert image, this type of image share generation can also be used to split a secert password or a key between stake holders of equal level and can act as a binding condition for decryption in confidential key/secret holding users.

VII. Conclusion

A *(n, n)* secret sharing scheme provides for binary image, gray scale image and a RGBA image. In this paper we propose a new *(n, n)* secret sharing scheme, based on a bit wise XOR.The performance of the proposed scheme on the gray scale images is comparable to the existing schemes and the noise correction can be applied for correcting the image after retrieval and is negligible. The findings of our proposed scheme in color scale images raises new questions on the performance of this enhanced security architecture and is open for the research community in the future to share their findings. In the proposed scheme even if n shares are captured or hijacked, the secret cannot be retrieved due to added cellular automata encryption at each transparency layer. XOR operations are used in the *(n, n)* algorithm. The proposed (2, n) scheme is probabilistic and the contrast of the recovered image is better than the existing gray scale and binary schemes for jpg type image storage. The time complexity for the reconstruction of the shares is O(n) due to the bitwise xor operation used in the proposed scheme.Based on the Boolean operator XOR, the proposed scheme can easily recover the reconstructed image [6]. Our secret sharing can also be applied on color images but is not able to retain the transparencies. The Layer 1 of proposed scheme can be adjusted according to the level of security required by using more complex rules.

Our future work would be focused on improving this scheme for having a lossless share generation for the RGBA images and extend the image library to work with video encoding on the wire, using more faster hardware interfacing as boolean operators already have custom data paths for execution and would offer better performance when improved upon.

VIII. Acknowledgments

The authors express their gratitude to Department of Science & Technology (DST), India for the obtained financial support in performing this research work. This work is one of the outcomes of the project entitled “Secret Sharing Scheme based technology for multimedia security over cloud” with sanction no. DST/ICPS/Cluster/CS Research/2018 (General) dated 13.03.2019, sponsored by DST.

References

[1] Naor, M., and Shamir, A.Visual cryptography. InAdvances in Cryptology —EUROCRYPT’94(Berlin, Heidelberg, 1995), A. De Santis, Ed., Lecture Notesin Computer Science, Springer, pp. 1–12.

[2] Hou, Y.-C.Visual cryptography for color images.Pattern Recognition 36(072003), 1619–1629

[3] Youmaran, R., Adler, A., and Miri, A.An Improved Visual CryptographyScheme for Secret Hiding. In23rd Biennial Symposium on Communications,2006(May 2006), pp. 340–343

[4] Shivani, S., Rajitha, B., and Agarwal, S.XOR based continuous-tonemulti secret sharing for store-and-forward telemedicine.Multimedia Tools andApplications 76, 3 (Feb. 2017), 3851–3870.

[5] Shamir, A.How to share a secret.Communications of the ACM 22, 11 (Nov.1979), 612–613.

[6] B, R. K., K, N. K., and G.V.S, R. K.Secret image sharing technique basedon bitwise xor.IJCSET 6, 5 (2016), 138–143.

[7] S. Nandi, S. Roy, S. Nath, S. Chakraborty, W. Ben Abdessalem Karaa and N. Dey, ”1-D group cellular automata based image encryption technique,” 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kanyakumari, 2014, pp. 521-526, doi: 10.1109/ICCICCT.2014.6993017.

[8] J. K. Mantri, R. Mishra and P. Gahan, ”A Novel Encryption Scheme Using Hybrid Cellular Automata,” 2019 International Conference on Information Technology (ICIT), Bhubaneswar, India, 2019, pp. 382-387, doi: 10.1109/ICIT48102.2019.00074.

[9] Verheul, E. R., Tilborg, H. C. (1997). Constructions and Properties of k out of n Visual Secret Sharing Schemes. Designs, Codes and Cryptography, 11(2), 179-196. doi:10.1023/a:1008280705142

[10] C.-C. Thien and J.-C. Lin, ”Secret image sharing”, Comput. Graph., vol. 26, no. 5, pp. 765-770, Oct. 2002.