# Army Data Encode Using Visual Cryptography

[1]M.V.R. NIKHIL, [2]SHIV SHANKAR SINGH, [3]B. NIKHIL, [4]K. SAI SANKAR, [5]D. SAI GANESH PATNAIK, [6]G. JAGADISH

[1,2,3,4,5] Student, [6]Asst. Professor, Dept. of CSE, Anil Neerukonda Institute of Technology and Sciences, Visakhapatnam, Andhra Pradesh, India. [1]mvr.nikhil@gmail.com, [2]sshivshankar9850@gmail.com, [3]bommalatanikhil@gmail.com,[4]kurmalasankar4200@gmail.com, [5]ganeshpatnaik95@gmail.com, [6]gjagadish.cse@anits.edu.in

***Abstract*: In any army a decision is not directly taken by just one commander or leader but rather that same decision is taken only after discussing about that issue and a majority agrees upon it. This had become the base idea of our paper. In this paper, the idea was to secretly transmit a secret image which can possible be any kind of important map or as such to the main people in the army and the original image can be formed only when the required number of people agree to that plan. This is done by the concept called "Visual Cryptography". Visual Cryptography deals with images. Visual cryptography is a technique which allows visual information such as images ,videos etc. to be encrypted in such a way that the decrypted information appears as a visual image .In this paper we implement visual cryptography on black and white images and colour images(RGB) using "(k , n) secret image sharing algorithm" .This scheme is perfectly secure and very easy to implement. We extend this algorithm in such a way that the secret image is divided into n shares and each share is sent to n different officers and only when at least k officers (k<=n) agree to see the secret and when they combine their individual share, the secret is revealed.**

***Keywords*: bitwise OR, cryptography, decryption, encryption, k out of n shares, (k, n) secret sharing algorithm, RSA, shares, visual cryptography.**

## I. INTRODUCTION

Image Processing is a process of working with images and extracting useful information out of it. Visual Cryptography is one variant of Image Processing where we hide the secret image so that it is not visible as it has to be but as a different image.

Visual cryptography is the method of hiding images or documents by shadowing the original image into specific shares which are visually not recoverable. A secret is something which is kept from the knowledge of any but the initiated or privileged. Secret sharing denies a method by which a secret can be distributed between a group of participants, whereby each participant is allocated a piece of the secret. This piece of the secret is known as a share. The secret image can only be reconstructed when a sufficient number of shares are combined together. While these shares are separated, no information about the secret can be accessed. That is, the shares are completely useless while they are separated. These shares when superimposed on one another would give away the concealed image. Here, we are going to use the scheme of [3],[10] (k, n) secret sharing algorithm. This visual cryptographic scheme consists of 'n' participants. For the image that has to be recovered, we create 'n' shares of that secret image which is visually not recoverable if seen individually. Now, each of these 'n' participants is handed over a share. These share when stacked over one another would reveal the hidden image. Hence, each of the participants would hold the secret but won't be able to decode it unless k people come by and gives their individual share. [1] Naor and Shamir (1994) introduced this cryptographic paradigm for black and white images. The analysis was carried on a k out of n scheme, where n is the number of shares created and k is the minimum number of shares that needs are to be stacked to recover the hidden image. That is if fewer than k shares are stacked together, the image would still remain unclear. Within a secret sharing scheme, [2],[3],[10] the secret is divided into a number of shares and distributed among n persons. When any k or more of these persons (where $k \leq n$) bring their shares together, the secret can be recovered. However, if k - 1 persons attempt to reconstruct the secret, they will fail. Due to this threshold scheme, we typically refer to such a secret sharing system as a (k, n)-threshold scheme or k-out-of-n secret sharing.

## II. LITERATURE SURVEY

The basic idea of secret sharing was introduced by [1]Shamir in the year 1994 in his paper "How to Share a Secret?" where a data D is divided into 'n' shares/pieces in

 DOI : 10.35291/2454-9150.2020.0193 

such a way that 'D' can be easily reconstructed from any of the 'k' out of those 'n' shares/pieces, but the knowledge of at most 'k-1' pieces cannot reconstruct 'D'. This was implemented by the concept of [6] 'Interpolation'. This idea was further developed into [3],[10]K-N Secret Sharing algorithm by using a Random Number where in each pixel value is being put in any of the 'n-k+1 shares'(reconstruction factor) out of the 'n' shares so that a particular pixel value is definitely found in at least one of the 'k' shares that are being selected. We also made use of the paper [2] "A Novel Approach on Secure Data Transfer for General Transactions using Secret Sharing Scheme". In addition to the above-mentioned algorithm, we introduced a cryptographic technique to encrypt the secret image and then divide it into 'n' shares. Later after combining 'k' shares we then need to decrypt the reconstructed image to get back the secret image. Here, in this paper we used a simple symmetric cryptographic algorithm (Caesar Cipher) along with a strong asymmetric cryptographic algorithm (RSA) to provide more security.

## III. RELATED WORK

All this had been started by [1] Naor and Shamir where they proposed the idea of k out of n secret sharing algorithm. This model assumes that the secret message is a collection of black and white pixels and each pixel is handled separately. Each original pixel can appear in 'n' modified versions called shares. Each pixel in original image is represented by a collection both while and black subpixels, which are printed close to each other on transparencies. This model only works for black and white images. Now when a min of 'k' shares is brought together and stacked one above the other, it gives out the original or secret image. [3],[4],[10] Later, this idea had been improved and made simple by using a random number generator. A reconstruction factor is first calculated(n-k+1). Now each pixel of the original image is put in (n-k+1) shares. This is done for a surety that no pixel of the original image gets missed when we select k shares out of the n shares. Human visual system acts as an OR function. So, having that pixel in at least one of the k shares is enough to have that pixel in the output. This algorithm works for black and white as well as RGB images.

## IV. METHODOLOGY

We are proposing a method that is quite easy and simple to implement. These are the steps of our proposed method.

1. An image that is to be secretly transmitted should be selected.
2. This selected image will then be encrypted,
   2.1 First by using Caesar cipher where in we make use of a key and compute a value. Then we add this value to all the pixels and mod it by 256.
   2.2 Then we use RSA encryption where in we compute a pair of public and private keys. Now with this public key, we encrypt all the pixel values using RSA.
3. Then we split this encrypted image into 'n' shares using [3] (k, n) secret sharing encryption algorithm.
4. Then we send each share to each individual person via mails.
5. Now, at least 'k' of 'n' shares are selected for merging.
6. Once the shares are selected, then we overlap and combine these shares using [3] (k, n) secret sharing decryption algorithm.
7. Once we got the merged image, then it is time to carefully decrypt the merged image.
   7.1 The decryption starts by decrypting using RSA. The private key that we generated earlier is used for RSA decryption.
   7.2 Next, we make use of the key (that we earlier used for Caesar Cipher encryption) for decrypting using Caesar Cipher.

This order must match with the reverse order in which encryption is done. If first encryption is Caesar Cipher, in decryption using Caesar Cipher has to be done last.

8. We will have the final image.

Finally, after all these steps we will be able to get the original secret image.

These are the modules that are being proposed:

### 4.1 Encryption

Encryption is that process where the data is transformed into an incomprehensible data that is not in its original format. Encryption is necessary to provide more security to the secret that is being transmitted so that even the shares are taken by the intruders, they cannot form the secret back to its original form. In this paper, we make use of 2 encryption algorithms: first one is a simple and easy symmetric encryption algorithm Caesar Cipher where in every value in each pixel is added with a fixed value(key) and then mod with 256 because every value in a pixel is in the range of 0-255, the next encryption used is a stronger algorithm RSA which makes use of two pairs of keys(public and private). Two encryption algorithms are used to make the security much stronger.

Time Complexity for Encryption:

1) Caesar Cipher Encryption: O(row*column*3)
2) RSA Encryption: O(row*column*3*log(e))

### 4.2 Division into 'n' Shares (n- share generation)

The encrypted image is used to perform share generation where the shares of the image is generated using [3],[4],[10] (k-n) secret sharing algorithm. This algorithm as name suggests makes use of n and k values to generate the shares of the image. In this algorithm a number of matrices equal to 'n' are created. Now each RGB value in each pixel is placed in any random (n-k +1) number of

 DOI : 10.35291/2454-9150.2020.0193 

matrices [5],[9]. As a result, each matrix does not hold information about all RGB values of pixels and at the same time holds enough information to be a share. After all the RGB values are placed now shares are generated based on these matrices.

Time Complexity for Division into 'n' shares:

1) Division into N-Shares: O(row*column*(N-K+1))

### 4.3 Generate and Send e-mails

Emails are sent to user's emails provided by admin. Here each user would be an army officer who are required to make a decision. The number of emails is equal to number of shares created at the first place. Now, each user will get a share of the secret image.

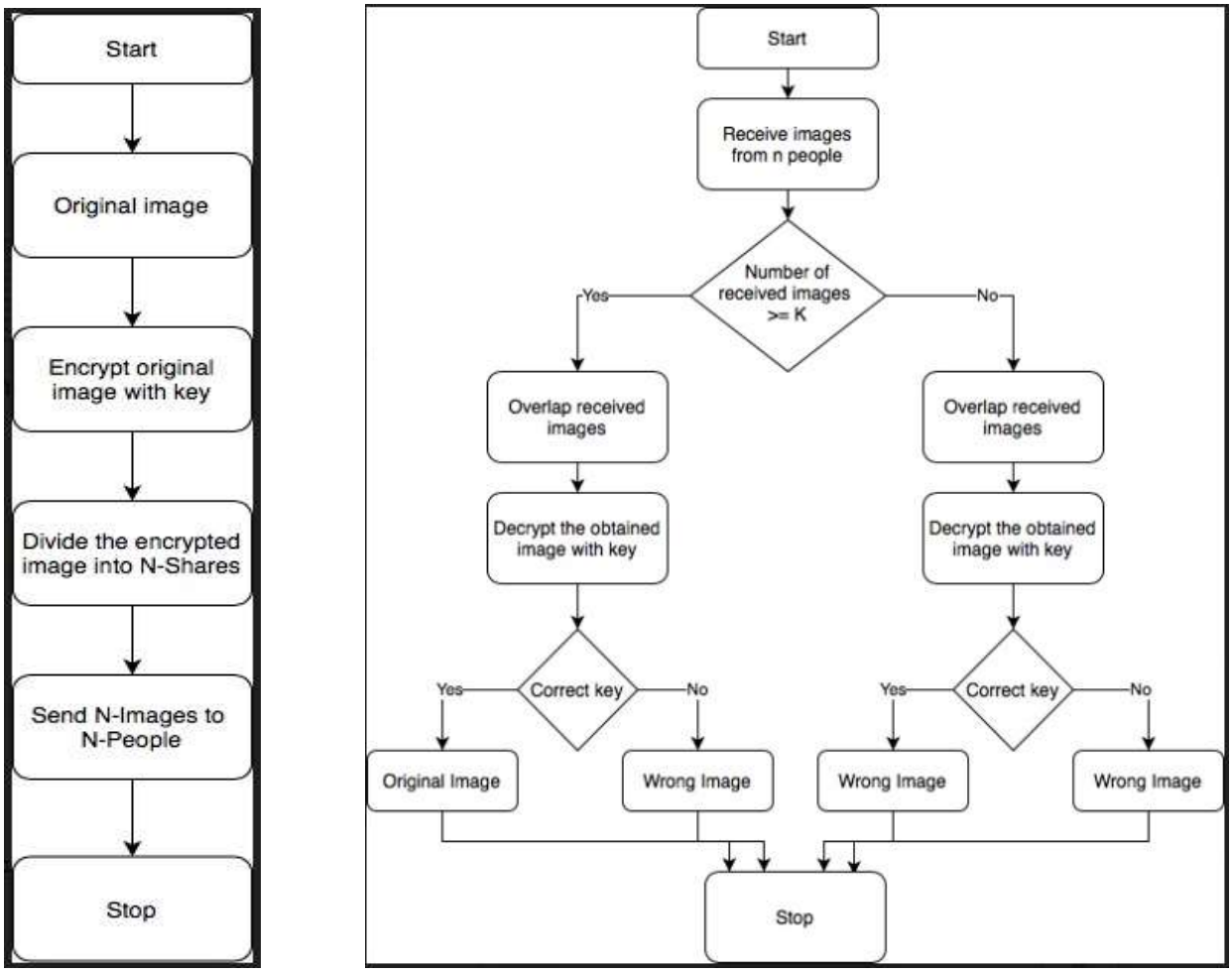


**Figure 1: System Architecture: a: Encryption and Dividing into 'n' shares.**
**b: Merging 'k' shares and Decryption.**

### 4.4 Overlapping k-shares

To reconstruct the image from n shares, at least k shares of those n shares are definitely required. Even though the knowledge of k-1 shares cannot form the original image. Now if at least k out of n users accept to contribute their shares, then the image can be reconstructed. Image is constructed from these shares based on OR operation so that every non-zero pixel is considered and used for image construction. As a result, the image is ready for decryption.

Time Complexity for Merging 'k' shares:

1) Overlapping K-Shares: O(K*row*column*3)

### 4.5 Decryption

The image reconstructed from shares is decrypted in this module. The reconstructed image is first decrypted using RSA algorithm. Now the resultant is then decrypted with a key using Caesar Cipher. These keys must be same or related to the ones that are used during encryption. Wrong key won't give us the original image back and secret won't be revealed properly.

Time Complexity for Decryption:

1) Caesar Cipher Decryption: O(row*column*3)
2) RSA Decryption: O(row*column*3*log(d))

 DOI : 10.35291/2454-9150.2020.0193 

## V. EXPERIMENTAL RESULTS

Jung-San Lee et.al suggested security, element enlargement, accuracy and procedure quality as a performance measure [7]. Security is glad if every share reveals no info of the initial image and also the original image can't be reconstructed if their square measure fewer than k shares collected. Accuracy is taken into account to be the standard of the reconstructed secret image and evaluated by peak signal-to-noise (PSNR) live. Procedure quality considerations the full variety of operators needed each to get the set of n shares and to reconstruct the initial secret image.

| File Name | Resolution (w*h) | Encryption Time (in sec) | Decryption Time (in sec) |
|---|---|---|---|
| anits.png | 200*200 | 0.2362 | 0.3569 |
| download.jpg | 225*225 | 0.2951 | 0.4969 |
| Flower.jpg | 159*119 | 0.1234 | 0.1837 |
| god.png | 450*450 | 1.1775 | 2.1045 |
| human.jpg | 208*243 | 0.2957 | 0.4895 |
| map.jpg | 300*168 | 0.3117 | 0.4938 |
| mona.png | 256*256 | 0.4669 | 0.6476 |
| tulip.png | 173*292 | 0.2989 | 0.4882 |

**Table-1: RSA Encryption and Decryption times for images with different resolutions.**

| File Name | Resolution (w*h) | Encryption Time (in sec) | Decryption Time (in sec) |
|---|---|---|---|
| anits.png | 200*200 | 0.1333 | 0.0980 |
| download.jpg | 225*225 | 0.1310 | 0.1270 |
| Flower.jpg | 159*119 | 0.0474 | 0.0677 |
| god.png | 450*450 | 0.6036 | 0.5164 |
| human.jpg | 208*243 | 0.1475 | 0.1214 |
| map.jpg | 300*168 | 0.1162 | 0.1286 |
| mona.png | 256*256 | 0.1364 | 0.1672 |
| tulip.png | 173*292 | 0.1157 | 0.1402 |

**Table-2: Caesar Cipher Encryption and Decryption times for images with different resolutions.**

| File Name | Resolution (w*h) | Time taken for dividing Image into 'n' shares (in sec) (n=5) | Time taken for combining 'k' shares to form the Image (in sec) (k=4) |
|---|---|---|---|
| anits.png | 200*200 | 2.3271 | 0.3847 |
| download.jpg | 225*225 | 2.7729 | 0.4426 |
| Flower.jpg | 159*119 | 1.8608 | 0.1910 |
| god.png | 450*450 | 6.3979 | 1.9212 |
| human.jpg | 208*243 | 2.6610 | 0.4559 |
| map.jpg | 300*168 | 2.6496 | 0.4583 |
| mona.png | 256*256 | 2.9356 | 0.6124 |
| tulip.png | 173*292 | 2.6486 | 0.4697 |

**Table-3: Time taken for Dividing an Image into 'n' shares and Combining 'k' shares to form an Image for images with different resolutions (n=5.k=4).**

**Figure 2: Input Image**

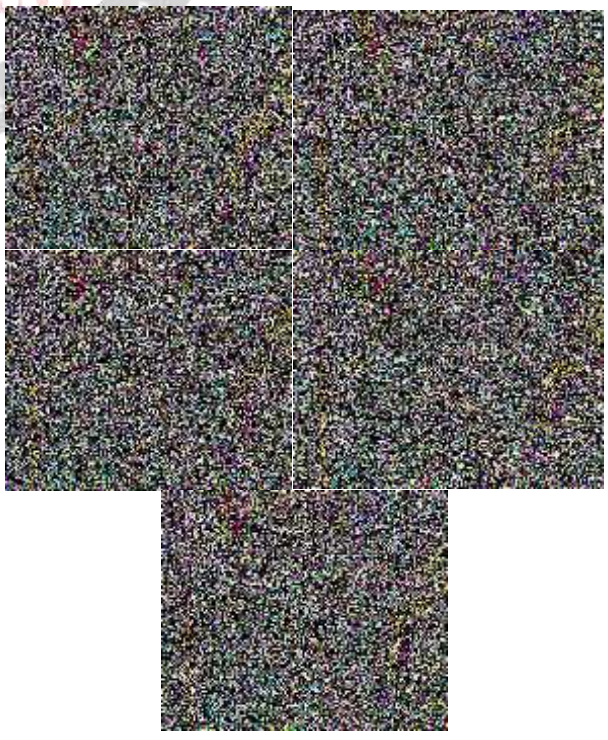

**Figure 3: Shares(n=5,k=3)**

 DOI : 10.35291/2454-9150.2020.0193 

**Figure 4: Output Image (Combining at least 4 shares)**

Peak Signal to Noise Ratio (PSNR) is the ratio between the maximum possible power of an image to that of the power of corrupting noise that affects the quality of its representation.

$$PSNR = 10log_{10}\left(\frac{(L-1)^2}{MSE}\right)$$

where, L in the maximum intensity level.

Mean Squared Error (MSE) is defined as follows,

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

where, O is the original image and D is the resultant image.

The image that is being recovered (by using the above method) after merging properly and decrypting properly is same as that of the original image and it is noise free. If at all, something is not done properly there will be noise and value of PSNR is computed by using the above formulae.

If MSE is zero, then there is no noise in the original image.

## VI. CONCLUSION AND FUTURE WORKS

Sharing data secretly, especially in the domain of army is very important. That data that is being transmitted is very sensitive. So, it is very important to transmit data by providing security to it. This idea not only makes it difficult for intruders to steal the data but also makes it nearly impossible as we encrypt the data before dividing into shares. Encryption provides extra security for the data in addition to that data being divided into shares. Now even if the intruder has required number of shares, he won't be able to get the original image as it is as he doesn't know the values of the key. What makes this algorithm good is that, the intruder has to get all the required number of shares at the first place and this is tough. What is tougher is that even if he has the required number of shares, he should have the key values as well. So, its better if the value of 'k' to be closer to the value of 'n' and also have a good set of keys for encryption.

This proposed method has a compulsion that there should be only one admin and the each shareholder has to take the shares from and has to bring back the shares to that only admin. It is that person who initially takes the image to be shared secretly, encrypt the image, divide into 'n' shares, send mails, combine the accepted shares, decrypt the image, get back the secret image and maintain all the files related to that image. It can be further extended in such a way that encryption, division into 'n' shares and mailing those shares be done at one end taken care by one admin and combining 'k' shares and decryption be done at another end taken care by another admin. This makes this algorithm more feasible and robust to use and work with. Also, with the changing technologies, newer and stronger encryption algorithms can replace the ones that are used in this proposed algorithm.

This same idea can be used in other fields as well like in providing authentication in Photography Contests, Online Voting Systems using Visual Cryptography, in Copyright authentication etc.

## REFERENCES

[1] Adi Shamir "Communications of the ACM: How to Share a Secret" Volume 22, Issue 11 Nov. 1979.

[2] J. Sharmila, Jagadish Gurrala "A Novel Approach on Secure Data Transfer for General Transactions using Secret Sharing Scheme" International Journal of Computer Applications (0975 – 8887) Volume 172 – No.8, August 2017.

[3] Shyamalendu Kandar, Arnab Maiti "K-N SECRET SHARING VISUAL CRYPTOGRAPHY SCHEME FOR COLOR IMAGE USING RANDOM NUMBER" International Journal of Engineering Science and Technology (IJEST).

[4] Moni Naor, Adi Shamir "Visual Cryptography" (The preliminary version of this paper appeared in Eurocrypt 94).

[5] Jagadish, et al., "A Secure Framework for Communicating Multimedia Data in Cover Images using Hybrid Steganography Algorithms in Wireless Local Area Network", published Scopus journal in International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-9 Issue-2S3, December 2019.

[6] A. Kalai Selvi, Dr. M. Mohamed Sathik, "Polynomial Based Secret Sharing Scheme for Image Encryption Based on Mathematical Theorem" Volume 2, No. 1, Jan-Feb 2011 International Journal of Advanced Research in Computer Science.

[7] Jagadish, P Sanyasi Naidu, published paper "Scalable Methodology to Hide Audio Data in Cover Image using RGB and Grey Colour based Key Positioning Image Steganography", IJRTE, ISSN: 2277-3878, Volume-8 Issue-3, September 2019.

[8] P. Sanyasi Naidu, Reena Kharat "Secure Authentication in Online Voting System Using Multiple Image Secret Sharing".

[9] Jagadish Gurrala, Dr.P. Sanyasi Naidu, "Analysis of Existing Text Hiding Algorithms for Image Steganography Using TLNUS and AES", Smart Computing and Informatics, Proceedings on SCI 2016, Volume 7, pp © Springer Nature Singapore Pte Ltd. 2018, Systems and Technologies 77, https://doi.org/10.1007/978-981-10-5544-7_1, Dec 2017.

[10] Debashmita Poddar "(2, N) VISUAL CRYPTOGRAPHIC SCHEME FOR BLACK AND WHITE PIXELS USING SQUARE MATRICES" INDIAN STATISTICAL INSTITUTE, Kolkata, July 2016.

 DOI : 10.35291/2454-9150.2020.0193 