CYBER SECURITY
CSE4003
2019

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

ENCRYPTION OF GRAYSCALE IMAGES USING VISUAL CRYPTOGRAPHY WITH THE APPROACH OF BIT PLANE SLICING

SUBMITTED TO

SUDHA M.

SUBMITTED BY

ALOK SINHA	**17BCE2380**
MANISH PAIKARA	**17BCB0141**
BIBEK SINGH	**17BCE2393**

1. ABSTRACT

Contrasted with customary strategies, Visual Secret Sharing techniques for encryption help in accomplishing a high level of privacy and dependability. Secret sharing plans are perfect for putting away data that is exceptionally sensitive and critical. In this paper we present a novel technique for making shares of a grayscale picture by first isolating the picture into relating bitmaps. Making bit-plane cuts or bitmaps of a grayscale picture gives an additional degree of security to it. The multiple shares are formed by encoding where images are distributed into 'n' shares. With the idea of hiding secrets of shares of images by encrypting and decrypting the images with certain tools and algorithms. As indicated by this approach, first the grayscale picture is separated into 8 bitmaps and afterward 2 shares of each bitmap are created; all the primary shares are joined to produce 1st final share and all the second shares of each bitmap are consolidated to create final 2nd share. For the recreation of unique picture last offer 1 and last share 2 are consolidated.

2.PROBLEM STATEMENT

The problem prevails the high security propose, the grey scale image is distinguished into various division. The grey scale is less attractive which is one of the reasons for the attacker for not attacking and it becomes more secure. This system is used in the banking purpose and different area like the people who sends secret images from a restricted area. For example, news photographers or different spies who work in sensitive areas may send collected images to their companies or governments and many others. The main reason behind this is each slice of image is a general image so no one can detect that it contains some special encrypted message.

3. INTRODUCTION

Another type of cryptographic plan, which can decrypt concealed images without any cryptographic computations. This type is perfectly secure and very simple to execute. We broaden it into a visual variant of the k out of n secret sharing issue, in which a dealer gives a transparency to every one of the users; any k of them can see the image by stacking their transparencies, however (k – 1) of them gain no data about it. the original message is visible, if any (k) of them are kept together, but totally invisible and undetectable if fewer than k transparencies are stacked together. a black pixel is translated in the reconstruction into a black region while a white pixel is translated into a grey region.

Digitally, a picture is represented in term of the pixels it contains. These pixels can be expressed further in terms of bits. In the event that a grayscale picture is viewed as, every pixel comprises of 8 bits. Here, plane 0 contains the most reduced request bit of the considerable number of pixels in the picture and plane 7 contains the most noteworthy request bit of the considerable number of pixels in the picture. For any X-bit per pixel picture, cutting the picture at various planes (bit-planes) assumes an essential part in the region of picture preparing. A use of this system is information compression. As a rule, 8-bit per pixel pictures are handled. A picture can be cut into the accompanying piece planes. Zero is the minimum critical piece (LSB) and 7 is the hugest piece (MSB). Grayscale advanced pictures can be thought of as a network of pixels with forces (values). In an 8-bit picture, these qualities run from 0 to 255.

4. LITERATURE REVIEW

[1]. Visual Cryptography in Grey Scale Images

Visual Cryptograph is the new technique to secure the images by encrypting them with standard algorithms. In this method the images are divided into parts called shares and then they are distributed to the participants. The Grayscale images has the value of each pixel as a single sample that carries only intensity information that composed of shades of gray, varying from black at the weakest intensity to white at the strongest. The process applied to the gray scale image at the initialization phase and applying bit plane coding to form eight binary image and applying the concept of visual cryptography to all image bits and combining them to form actual image. Somewhat plane of a picture is a paired picture that conveys visual data of unique pictures in order to hold the first pixel esteems the equivalent when encryption. In visual cryptography if an individual gets adequate k number of offers; the picture can be effectively decrypted. This paper builds up an encryption technique to develop grayscale VC plot with utilizing bit plane encoding.

[2]. Visual Cryptography based Grayscale Image Watermarking in DWT domain

Watermarking is the way of implementing the possible data like image, audio, video, etc to be protected from the user’s right. It’s a task of encapsulating the data or abstracting the data using Visual Cryptography. Different algorithms and techniques can be generalized to bring this into effective way like Digital Watermarking, Discrete Wavelet Transform, Copyright Protection. The water making techniques categorized into spatial domain and frequency domain or transform domain techniques. Here the Visual Cryptography splits the images into unintelligible images which are called shares which again distributed to ‘n’ participants, so part of n the ‘k’ shares recover no information about secret. The secret image is obtained by the arithmetic XOR operation. The scheme satisfies about the Grayscale image helps in robustness, imperceptibility, blindness and security properties.

[3]. Multiple-Image Encryption by Rotating Random Grids

Visual Secret Sharing is the technique of encrypting a secret image into several share images which later on decrypts the secret by stacking the share images by constructing random grids. The random grids compared with the Visual Cryptography include no pixel expansion with sophisticated codebook design. Here the two secret images are engaged to two random grids without any pixel expansion. The gained secret images can be recovered by stacking two cipher-grids directly in two ways. With the simulation experiments converting the secret image into binary secrets to 90-degree rotation and halftone secrete 90-degree rotation. This obtained multirotational with varying dimension of new multiple-image scheme by rotating two random grids without any pixel expansion and codebook redesign. This multi-image Encryption helps to adopt the frequency and bandwidth of the encrypted and decrypted images.

[4]. Extended visual cryptography for natural images

This type of cryptography encodes a number of images the way where the images on transparencies are stacked together, the hidden message appears without a trace of original images. This visual cryptography system takes three images as input and generates two images which corresponds and reflect the combination of the rest three images. The extended means reconstructing the image by stacking them together. The process is non-periodic and dot-dispersed algorithm an extended visual cryptography scheme for natural images. It extends the concept of error and by performing the half toning and encryption simultaneously. The method of CFR is adopted in order to optimize the image quality better.

[5]. Encryption-then-Compression Systems using Grayscale-based Image Encryption for JPEG Images

The encryption is based on the enchanting the security of Encryption followed by Compression system with the extension of JPEG format. This will ensure the transmission of images through an untrusted channel provider, such as network provider. The proposed scheme enables the utilization of smaller block size and a larger number of blocks than conventional scheme. The method of block size enhances the robustness against cipher-text attacks. Images can be saved from the attacker in sense of using small block. The proposed scheme is applicable to SNS providers and cloud photo services like Tumblr, iCloud and Google photos. This technique avoids the effect of the interpolation on social media due to use of grayscale-based images.

[6]. Survey of Visual Cryptography Schemes

Visual Cryptography scheme is a cryptographic technique that helps to visualize the information in different formats like printed text, handwritten notes, and picture. This method of encryption in such a way that decrypting the same text is valuable from the attackers by the human visual cryptography. Different parameters like pixel expansion, security, accuracy, computational complexity, are meaningful for the encryption process. This intend to manage somehow to help in the process of different encrypting and decrypting algorithms. For avoiding the attention and making the less descriptive about the hackers are avoided. The visual cryptography enhances the share at a time to share multiple secret images numerous shares have to be generated. To determine the complexity of the multimedia information of gray or colour image format by measures such as frequency, security, contrast, etc by efficiency of visual cryptography.

[7.] Visual cryptography for gray-level images by dithering techniques

A(k-n) limit visual cryptography plan is proposed to encode a mystery picture into n shadow pictures, where any k or a greater amount of them can outwardly recoup the mystery picture, yet any k-1 for less of them gain no data about it. The translating procedure of a visual cryptography plot, which contrasts from customary mystery sharing, does not need muddled cryptographic instruments and calculations. This plan has the upsides of acquiring any created cryptographic procedure for double pictures and having less increment of picture size in conventional circumstances. The decoded pictures can uncover most subtleties of unique pictures. another visual cryptography plot reasonable for dim level pictures is proposed.

[8.] Bit-level based secret sharing for image encryption.

A new secret sharing scheme fit for protecting image data coded with B bits per pixel is introduced and analyzed in this paper. The proposed input-agnostic encryption solution creates B-bit shares by combining bit-level stacking with a [k, n]-threshold sharing strategy. Perfect decryption is done by performing decryption through simple logical operations in the decomposed bit-levels without the need for any postprocessing operations. The method proposed here (i) it uses bit-level decomposition for encrypt and stacking method to decrypt B-bit image, (ii) it saves every quality of traditional [k, n] sharing method, (iii) responsible for perfect decryption of the encrypted image by input B-bit image, (iv) encrypt binary, gray-scale and coloured pic, and (v) can be executed in both software or hardware.

[9.] Visual Cryptography

Another type of cryptographic plan, which can decrypt concealed images without any cryptographic computations. This type is perfectly secure and very simple to execute. We broaden it into a visual variant of the k out of n secret sharing issue, in which a dealer gives a transparency to every one of the users; any k of them can see the image by stacking their transparencies, however (k – 1) of them gain no data about it. the original message is visible, if any (k) of them are kept together, but totally invisible and undetectable if fewer than k transparencies are stacked together. a black pixel is translated in the reconstruction into a black region while a white pixel is translated into a grey region.

[10.] An improved Halftone Visual Secret Sharing Scheme for grey-level images.

It is based on error diffusion in forward and backward direction Visual cryptography is information security procedure which enables visual data to be encoded in such a way that their decryption can be performed by human visual framework. Visual secret sharing plan encrypts a secret image into certain shares which independently reveals no idea about the secret data. The visible image is first changed into halftones shares utilizing halftone error diffusion technique. Then secret image is encrypted into halftone shares carrying significant visual data. visual secret sharing plan by applying a new error diffusion filters that gives mistake in both forward and reverse way to increase the visual quality of the decoded secret image in VCS. practical shows that the decoded image is obtain by using proposed error diffusion filter is much better than previous error filters and this error filter gives maximum values for PSNR, NCC, UQI than other error filters.

[11.] A New Simple Non-Expansion Algorithm for (2, 2)-Visual Secret Sharing Scheme.

Visual cryptography is a incredible encoding method which combines perfect secrecy and secret sharing in cryptography as for the images. VC takes a binary image i.e. the secret and divides it into two or more parts. When the shares are stacked one over another, the secret image can be decoded. Visual cryptography is a most secure method that encrypts a secret image into different shares and the reconstruction of the image is by stacking the shares one over other. Unfortunately, this system leads to the decrease in the quality of the decrypted images and in image size expansion. In this paper, we apply a non-expansion algorithm for (2, 2)-VSS plan which resolves the problem of size expansion. The main aim of this plan is to encrypt the secret image in 4-pixel blocks with each and every block are assigned to a 4-pixel block in which each of the two shares as the number of white pixels in the block.

[12.] Sharing and hiding secret images with size constraint.

The method is new version which is taken from the (t, n) threshold scheme. The given encrypt image is sent and n shadow images are generated from which we can again decrypt the original image. Each shadow image is an ordinary image so as not to attract an attacker's attention. The size of each hidden image is about 1=t of that of the secret image, preventing the need for much memory space and transmission time. Experimental results indicate that the qualities of both the encrypt and decrypt images are about same. This idea is affective for the people who sends secret images from a restricted area. For example, news photographers or different spies who work in sensitive areas may send collected images to their companies or governments. Using this idea, they can easily share secret images into various smaller hidden images.

[13.] An Improved Image coding rule supported Chaotic System.

This coding rule relies on previous rule and is improved by analysing the principle of the chaos coding rule supported logistical map. Moreover, the protection and performance of the planned rule is additionally calculable. The experimental results supported coupled chaotic maps approve the effectiveness of the planned methodology, and also the coupled chaotic maps show blessings of enormous key area and high-level security. The ciphertext generated by this methodology is that the same size because the plaintext and is appropriate for sensible use within the secure transmission of counselling over the web.

[14.] A Visual Cryptographic Technique to Secure Image Shares

Visual Cryptographic Technique encrypts image by breaking it down into shares. It decrypts the image by overlaying the shares on top of each without any computation. This approach embeds visual cryptographically generated image shares in the host image using digital watermarking. This allows secret share to be generated which are digitally watermarked beneath a host image. The host image is then sent as share to recipients. The share image themselves have to be decrypted from their host as they are digitally watermarked there. These share files are then again overlapped to form the originally encrypted image. This method allows user to double the security on the image allowing for better security.

[15.] An Application of Visual Cryptography to Financial Documents.

One of the most important application of visual cryptography is transmitting financial documents where we need moderate security. Visual cryptography uses simple algorithm, no any complex algorithm is required. The visual cryptography solves the problem by decoding results in a grey version of the source document. Therefore, when visual cryptography is applied to financial documents or banking area, it is very difficult for the attacker to find digits accurately, it an unattractive protection technique due to which most of the attacker are not attracted towards it. visual cryptography requires increased storage due to the multiple transmissions, this algorithm, decreasing storage costs and overcome the existing problem, and make transmission fast.

[16] Image hatching for visual cryptography

Image hatching (or no photorealistic line-art) may be a technique wide employed in the printing or engraving of currency. numerous sorts of brush strokes have antecedent been adopted for various areas of a picture to make aesthetically pleasing textures and shading. as a result of there's no continuous tone among these sorts of pictures, a construction theme is planned, that uses completely different textures supported a intensity. These textures area unit then applied to the various levels and area unit then combined to create up the ultimate hatched image. The planned technique permits a secret to be hidden exploitation Visual Cryptography (VC) among the hatched pictures. Visual cryptography provides a awfully powerful means that by that one secret will be distributed into 2 or a lot of items referred to as shares. once the shares area unit superimposed specifically along, the first secret will be recovered while not computation. conjointly provided may be a comparison between the first grayscale pictures and therefore the ensuing hatched pictures that area unit generated by the planned rule. This reinforces that the quality of the hatched theme is ample. The Structural Similarity index (SSIM) is employed to perform this comparison.

[17] Hierarchical visual cryptography for grayscale image

In this technology era, each sensitive knowledge should be secured. Visual cryptography may be a technique to cover the image-based secret. In visual cryptography the key image is encrypted in to shares and at cryptography facet all shares are superimposed with one another so secret is disclosed. The key feature of visual cryptography is that, no troublesome computation is required at cryptography facet to rewrite the key. during this paper we tend to are applying stratified Visual Cryptography theme on grey image rather than binary image. So, generated shares are grey share, not binary shares that are generated by the binary image. Here we tend to are mistreatment the new planned grey share generation formula for generation of n range of shares. Here original image is encrypted in to n range of levels thus security of original image is enlarged. At cryptography facet all n shares should need to participate to reveal the initial secret. Decrypted image has same size and higher visual quality then original secret image.

[18] A comprehensive study of visual cryptography

Visual cryptography (VC) could be a powerful technique that mixes the notions of excellent ciphers and secret sharing in cryptography therewith of formation graphics. VC takes a binary image (the secret) and divides it into 2 or a lot of items called shares. once the shares square measure written on transparencies so superimposed, the key will be recovered. No pc participation is needed, so demonstrating one in every of the characteristic options of VC. VC could be a distinctive technique within the sense that the encrypted message will be decrypted directly by the human sensory system (HVS). during this survey, we are going to summarize the most recent developments of visual cryptography since its origin in 1994, introduce the most analysis topics during this space and description this issues and doable solutions. Directions and trends for future VC work shall even be examined together with doable VC applications.

[19] Visual secret sharing scheme using grayscale images

Pixel growth and also the quality of the reconstructed secret image has been a significant issue of visual secret sharing (VSS) schemes. variety of probabilistic VSS schemes with minimum element growth are planned for black and white (binary) secret pictures. This paper presents a probabilistic (2, 3)-VSS schemes for gray scale pictures. Its element growth is larger in size however the standard of the image is ideal once it's reconstructed. the development of the shadow pictures (transparent shares) relies on the binary OR operation.

[20] A new steganographic method for colour and grayscale image hiding

In this paper, we have a tendency to gift a steganographic methodology for embedding colormap colour} or a grayscale image during a true colour image. 3 styles of secret pictures may be carried by the planned method: activity a colour secret image, activity a palette-based 256-color secret image, and activity a grayscale image during a true color image. Secret knowledge area unit protected by the standard crypto system DES. we have a tendency to compare the image quality and activity capability of the planned methodology with those of the theme in architect et al.’s scheme. in step with the experimental results, the image quality of the planned methodology is best than that of the architect et al.’s scheme. additionally, annotation knowledge may be hidden with the key image within the host image. The activity capability of the planned methodology is larger than that of alternative compared schemes. The experimental results show that the planned methodology could be a secure steganographic methodology that has high activity capability and smart image quality.

5. IMPLEMENTATION PLATFORM / TOOLS

A. MINIMUM HARDWARE REQUIREMENT

- CPU: Core 2 Duo/Athlon X2 or better
- RAM: 1.5GB
- Graphic Card: 512MB of Graphics Memory
- Storage: 12GB

B. SOFTWARE COMPONENTS

- Python
- MATLAB

Python Imaging Library (abbreviated as PIL): may be a free library for the Python artificial language that adds support for gap, manipulating, and saving many various image file formats. it's offered for Windows, mac OS X and UNIX.

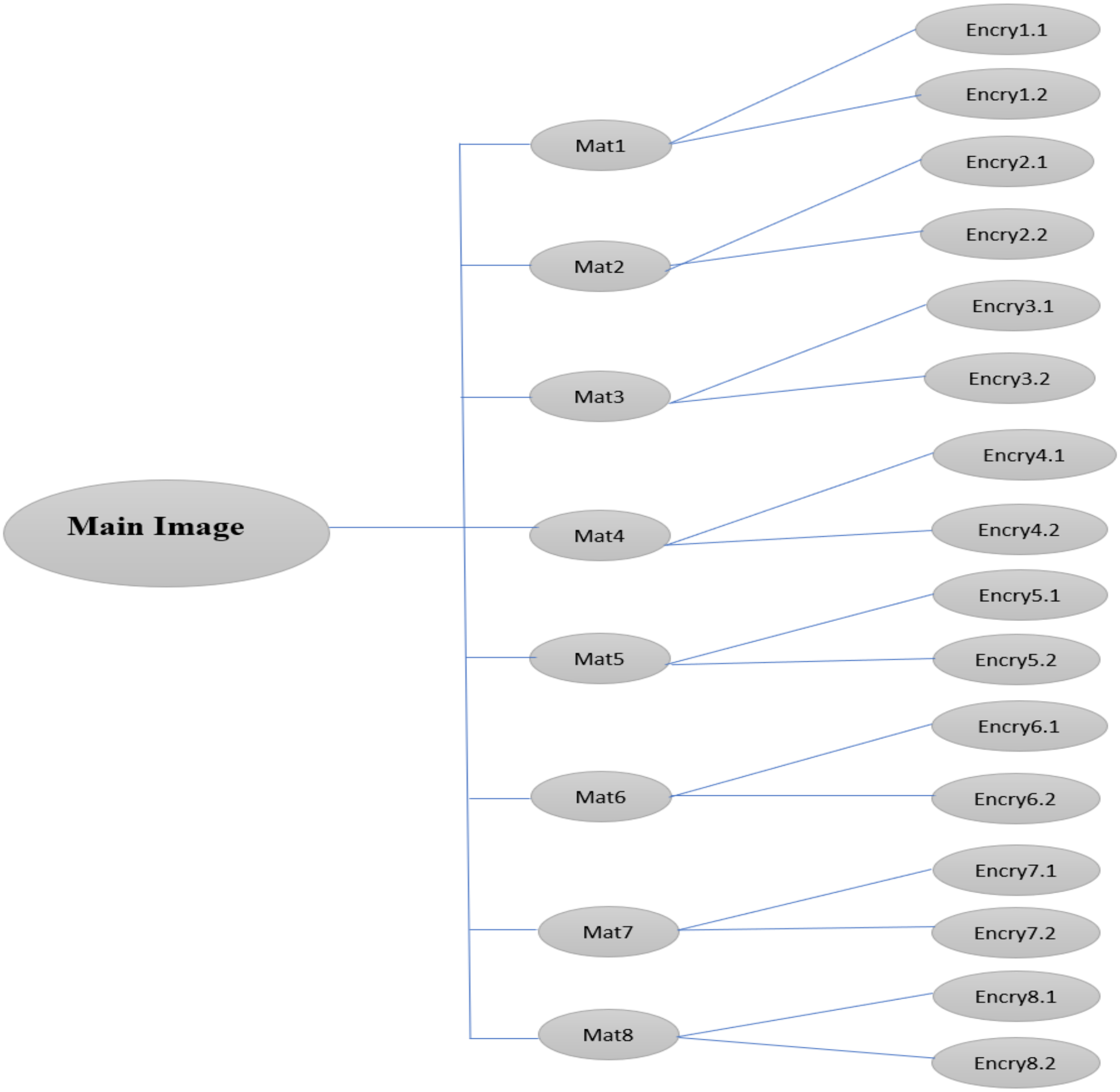
Pillow offers many normal procedures for image manipulation. These include:

- per-pixel manipulations,
- masking and transparency handling,
- image filtering, like blurring, contouring, smoothing, or edge finding,
- image enhancing, like sharpening, adjusting brightness, distinction or color,
- adding text to pictures and far a lot.

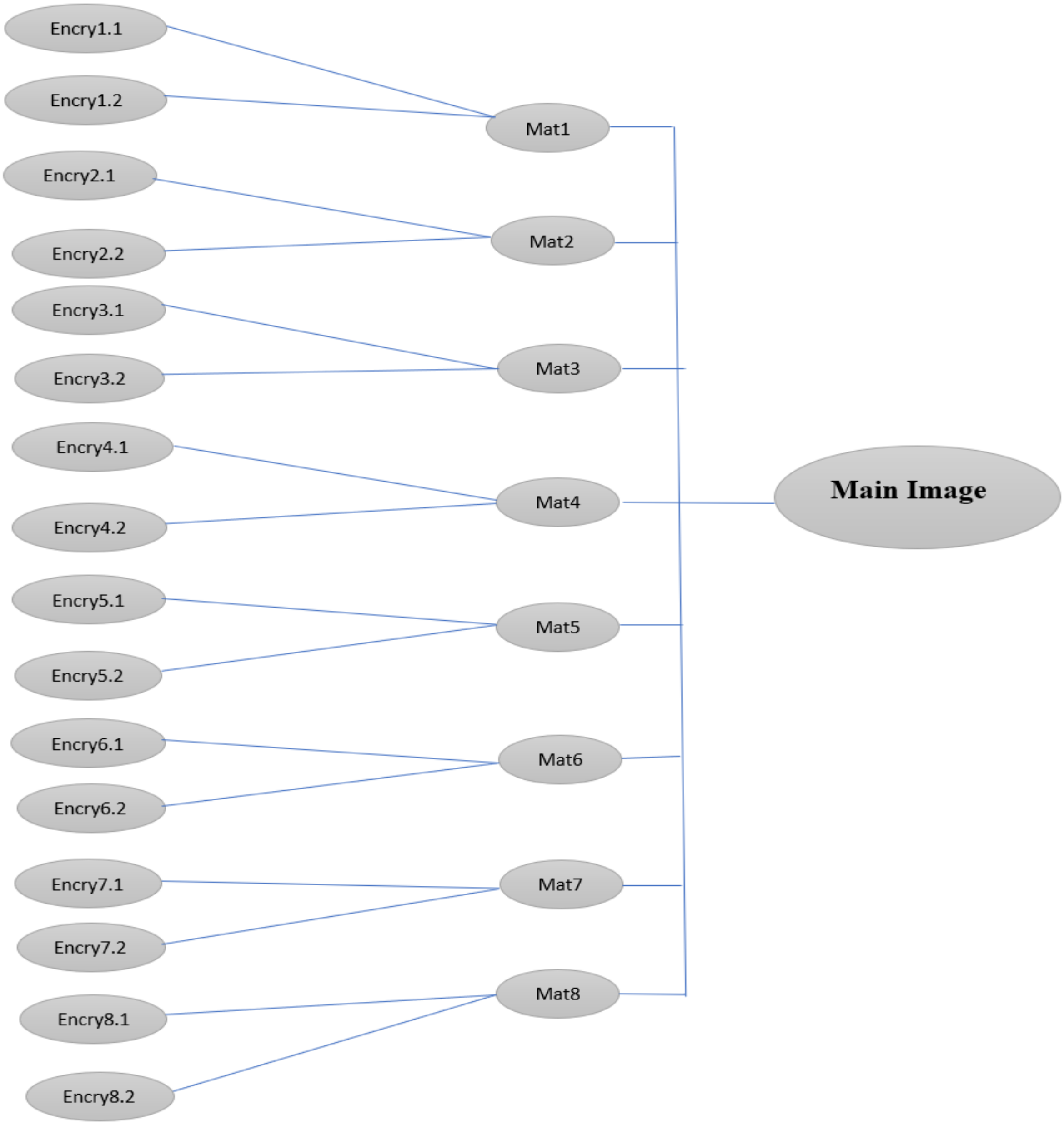
MATLAB for image cacophonic from grayscale to binary format for cacophonic and merging file to single when coding. MATLAB (lattice research facility) is a multi-worldview numerical processing condition and restrictive programming language created by MathWorks. MATLAB permits lattice controls, plotting of capacities and information, usage of calculations, making of UIs, and interfacing with programs written in different dialects.

In spite of the fact that MATLAB is expected fundamentally for numerical processing, a discretionary tool stash utilizes the MiPads representative motor enabling access to emblematic registering capacities. An extra bundle, Simulink, includes graphical multi-space reproduction and model-based plan for dynamic and implanted frameworks.

6. SYSTEM MODEL AND METHODS SYSTEM FLOW DIAGRAM



During the process of encryption, the Main Image is splitter into 8 images with respect to their bit size using MATLAB. After getting all 8-bit images we encrypt those images into 2 shares of each image bit. This will provide more security and for the decryption process the receiver have to get all the images as secret key and missing any one of the images will lead to failure in the decryption process.

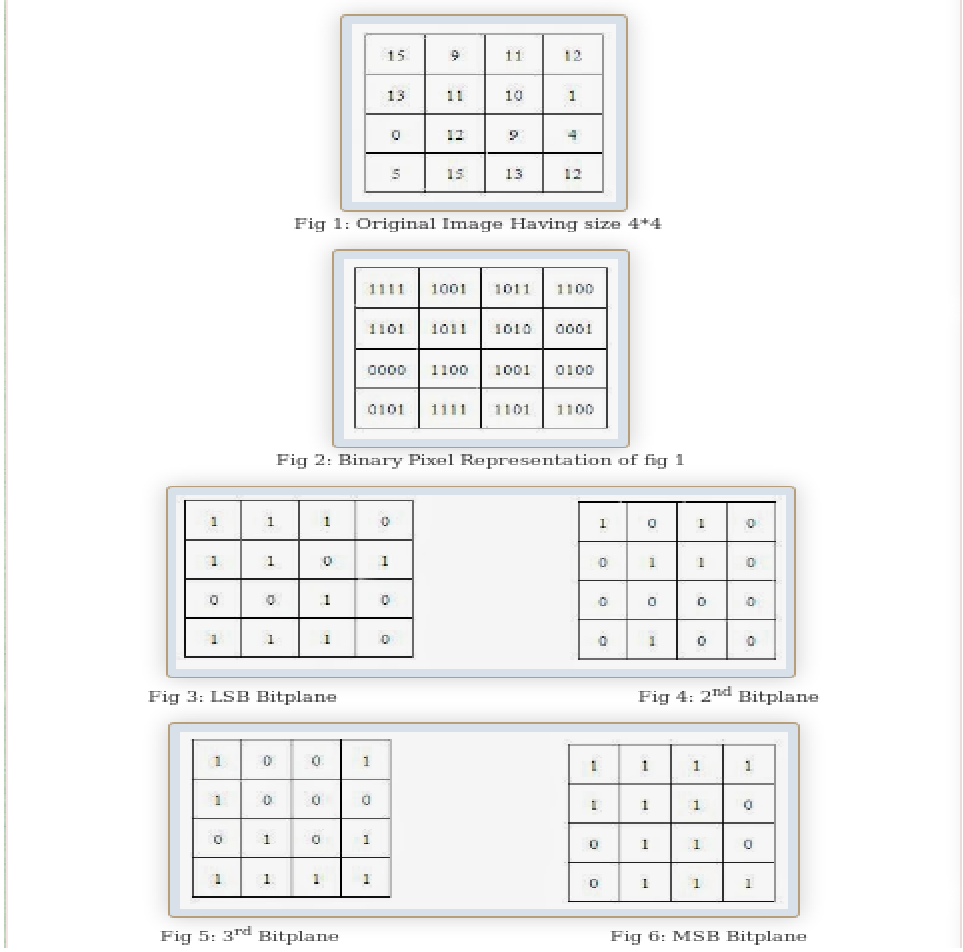


As the same method, for the message to decrypt we need all the 16 shares of the 8-bit images and after that the 16 shares are decrypted and converted into the 8 bit images and with the help of the MATLAB function and methods we finally get the same image. For the difference between the main image and the image we got after the process of encryption and decryption the hashing is done which will calculate the both images.

PSEUDOCODE OF ALGORITHM

- Start
- RGB to Gary-scale Conversion
    - Start
    - For each pixel = (red*0.29+green*0.59+blue*0.11)
    - Assign new pixel value to each pixel
    - Stop
- Bit-plane Splicing:
    - Start
    - For each pixel convert to binary
        - plane1 = mod(pixel,2)
        - plane2 = mod((pixel/2),2)
        - plane3 = mod((pixel/4),2)
        - plane4 = mod((pixel/8),2)
        - plane5 = mod((pixel/16),2)
        - plane6 = mod((pixel/32),2)
        - plane7 = mod((pixel/64),2)
        - plane8 = mod((pixel/128),2)
    - For each plane form an image according to original matrix
    - Stop
- Share Generation
    - Start
    - Map the pixels to 1 or 0 using function
    - pixels with 1 is saved as Share 1
    - pixels with 2 is saved as share 2
    - Stop
- Decrypt Share
    - Start
    - Open pair of shares
    - Tabulate pixels back to single image using decrypting function
    - Save as a single image
    - Stop
- Joining Bit Plane
    - Start

- For each pixel convert to binary
    - digit1 = mod(pixel,2)
    - digit1= mod((pixel*2),2)
    - digit3 = mod((pixel*4),2)
    - digit4 = mod((pixel*8),2)
    - diigit5= mod((pixel*16),2)
    - digit6 = mod((pixel*32),2)
    - digit7 = mod((pixel*64),2)
    - digiti8 = mod((pixel*128),2)
- Form an 8-bit number forming the original image
- Stop



15	9	11	12
13	11	10	1
0	12	9	4
5	15	13	12

Fig 1: Original Image Having size 4*4

1111	1001	1011	1100
1101	1011	1010	0001
0000	1100	1001	0100
0101	1111	1101	1100

Fig 2: Binary Pixel Representation of fig 1

1	1	1	0
1	1	0	1
0	0	1	0
1	1	1	0

Fig 3: LSB Bitplane

1	0	1	0
0	1	1	0
0	0	0	0
0	1	0	0

Fig 4: 2nd Bitplane

1	0	0	1
1	0	0	0
0	1	0	1
1	1	1	1

Fig 5: 3rd Bitplane

1	1	1	1
1	1	1	0
0	1	1	0
0	1	1	1

Fig 6: MSB Bitplane

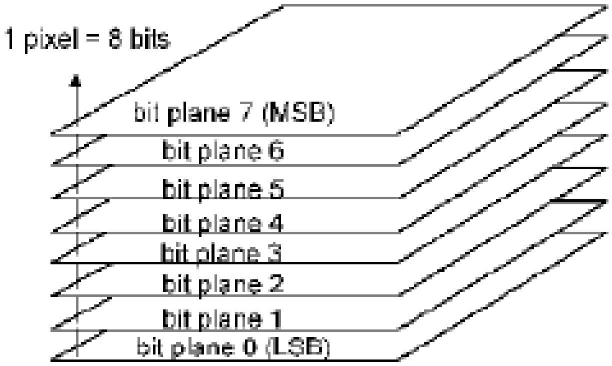
Fig: Bit Plane Splicing

7. PRE AND POST PROCESSING {SECURITY MECHANISM} OF MESSAGE FOR IMAGE INPUT

Visual cryptography and (k, n)-visual secret sharing schemes were introduced by Naor and Shamir in 1994.

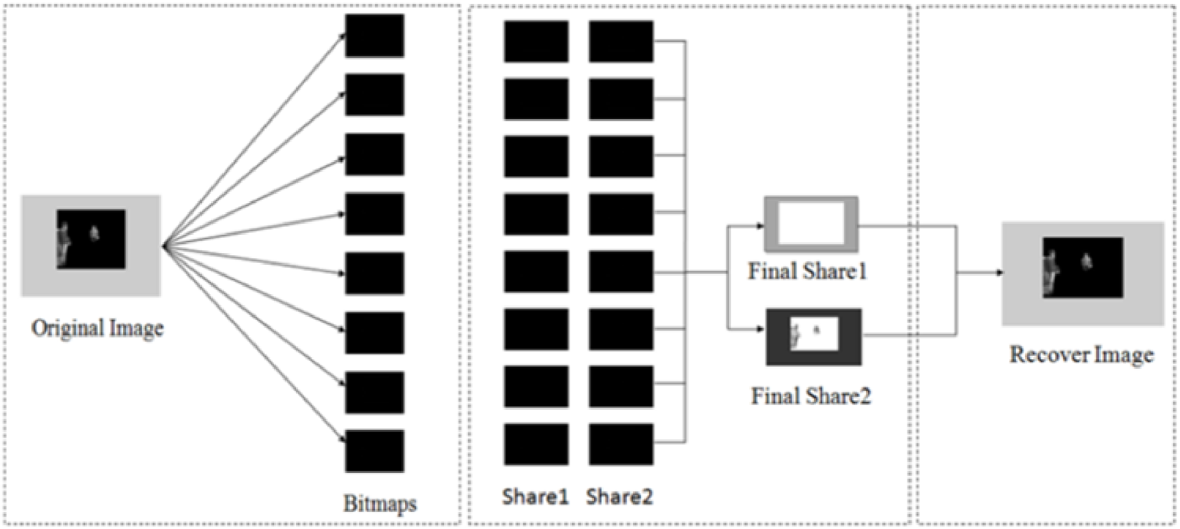
A. Bit-plane slicing

Digitally, an image is diagrammatic in term of the pixels it contains. These pixels are expressed additional in terms of bits. within the event that a grayscale image is viewed as, each constituent includes of eight bits. Here, plane zero contains the foremost reduced request little bit of} the sizeable range of pixels within the image and plane seven contains the foremost noteworthy request bit of the sizeable range of pixels within the image. For any X-bit per constituent image, cutting {the image} at numerous planes (bit-planes) assumes a vital half within the region of picture getting ready. A use of this method is data compression. As a rule, 8-bit per constituent footage square measure handled. an image is removing the incidental to piece planes. Zero is that the minimum crucial piece (LSB) and seven is that the largest piece (MSB). Grayscale advanced footage is thought of as a network of pixels with forces (values). In associate 8-bit image, these qualities run from zero to 255.



B. Share Generation

Here, we create two parts of each bitmap from the main bitmap up to the eighth bitmap. In this way, we get an aggregate of 16 shares, 2 each for each bitmap. To produce the two parts, we utilize the XOR activity on each piece.



The overview of our secure privacy-preserving scheme.

Bitmap 1:

$$\begin{bmatrix}0 & 1 & 0\\ 1 & 0 & 0\\ 1 & 1 & 0\end{bmatrix} = \begin{bmatrix}1 & 1 & 1\\ 1 & 1 & 1\\ 1 & 1 & 1\end{bmatrix} + \begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 1\\ 0 & 0 & 1\end{bmatrix}$$

Bitmap 2:

$$\begin{bmatrix}1 & 1 & 1\\ 0 & 0 & 1\\ 1 & 0 & 0\end{bmatrix} = \begin{bmatrix}1 & 1 & 1\\ 1 & 1 & 1\\ 1 & 1 & 1\end{bmatrix} + \begin{bmatrix}0 & 0 & 0\\ 1 & 1 & 0\\ 0 & 1 & 1\end{bmatrix}$$

$$\vdots$$

Bitmap 8:

$$\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 0\end{bmatrix} = \begin{bmatrix}1 & 1 & 1\\ 1 & 1 & 1\\ 1 & 1 & 1\end{bmatrix} + \begin{bmatrix}0 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 1\end{bmatrix}$$

Binary to Shares Matrix Representation

C. Reconstruction

To regenerate the original grayscale image, we combine all the first shares of every bitmap to create the final share 1 and similarly, all the second shares of every bitmap to create the final share 2. Then, the final share 1 and share 2 are combined using the bit-XOR operation to give the original reconstructed grayscale image.

8. Performance Evaluation Metrics

A. Bitmap creation

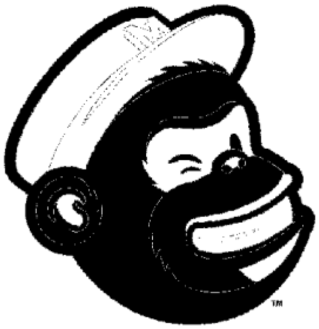
In this segment, cases are given to delineate the effectiveness of the proposed technique. Here, Figure is the original image which is converted to grayscale image and merging data to the Least Significant bits of the RGB image. This image is particularly a steganographic ally encrypted image in a grey scale format.

From Original image the eight bitmaps are created which are shown in Figure below

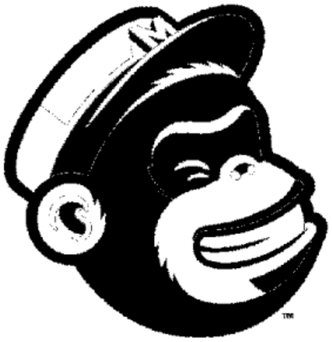
Bit plane 1

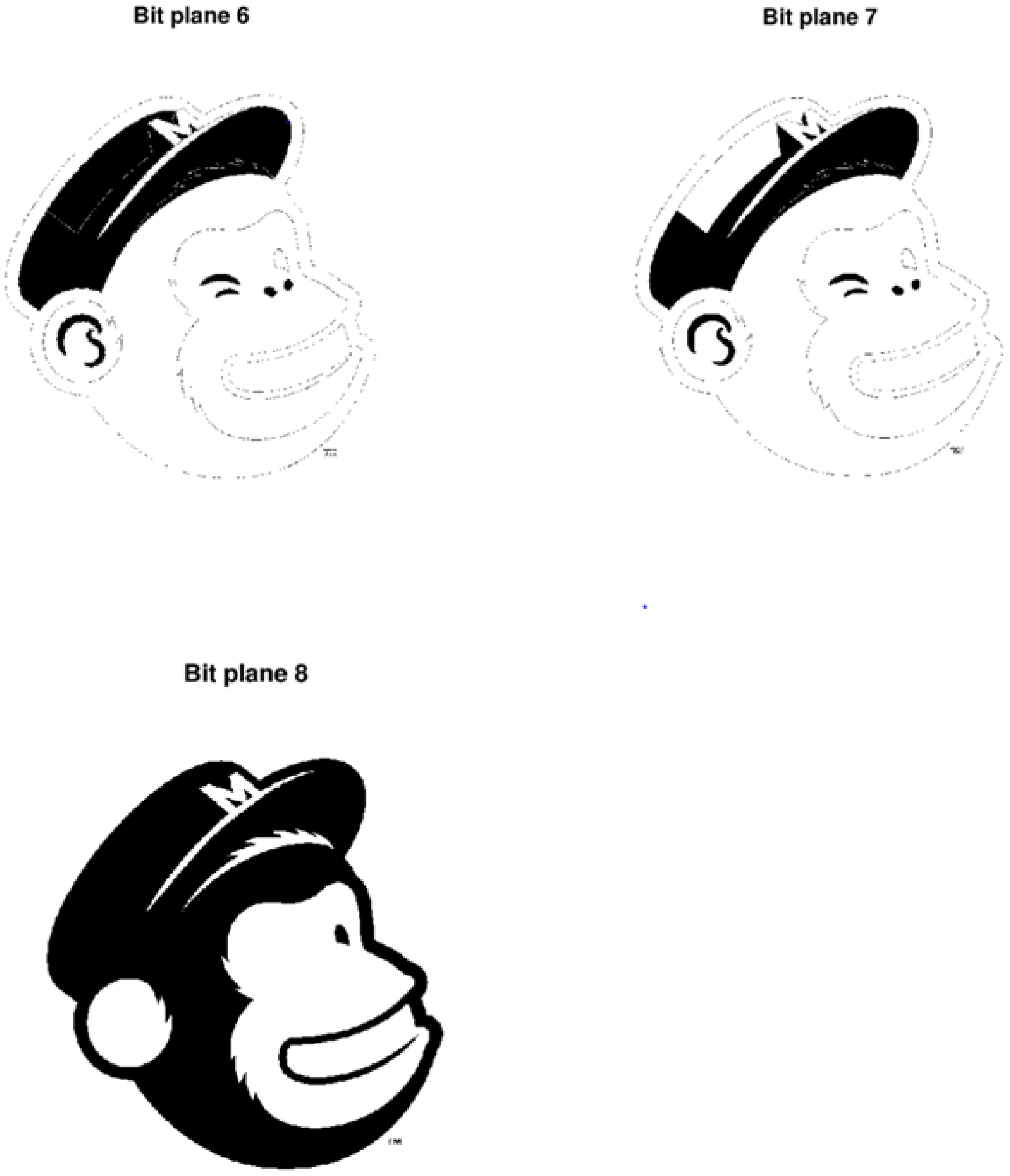
BITMAPS

Bit plane 2



Bit plane 3





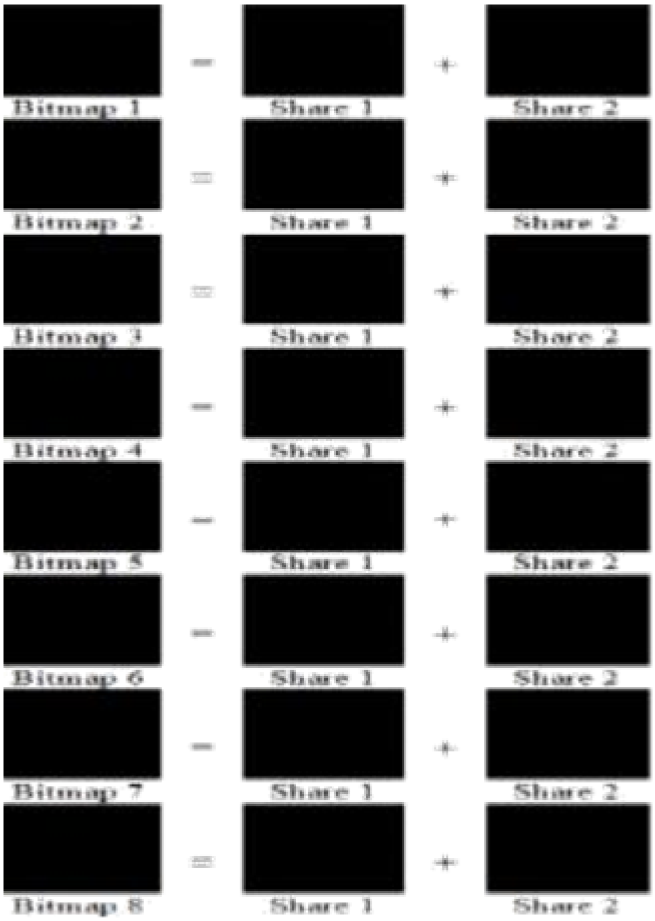
Bit plane 6

Bit plane 7

Bit plane 8

B. Share generation

After bitmap creation, two shares for each bitmap is created which as an example is shown in Figure below.



Share Generations

For creating the *Final share 1*, combination of all share 1’s and for *Final share 2*, combination of all share 2’s of eight bitmaps. *Final share 1* is shown in Figure

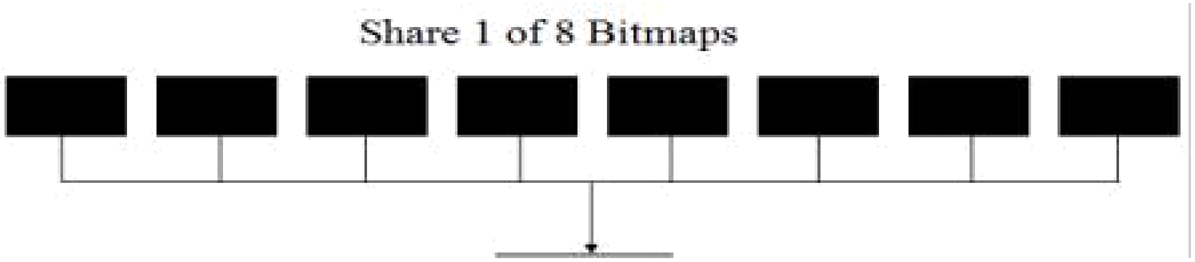
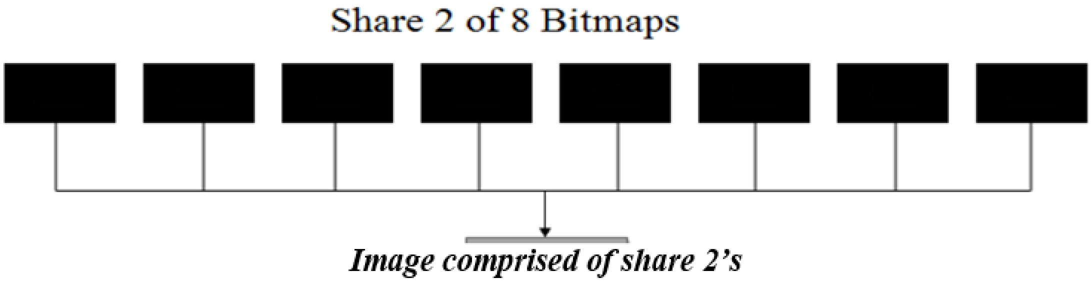


Image comprised of share 1’s

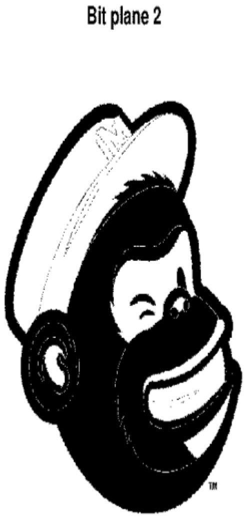
share 2 generations Figure is:



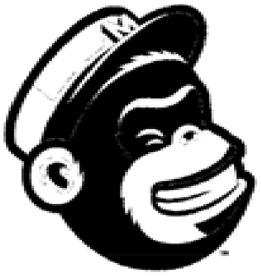
C. Reconstruction

Final generated images out of the share

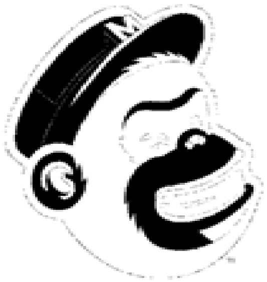
Bit plane 1


Bit plane 2

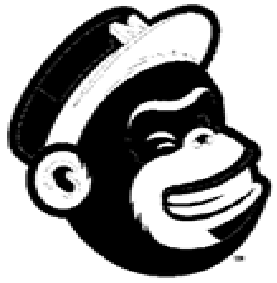
Bit plane 3



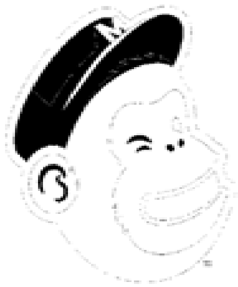
Bit plane 4



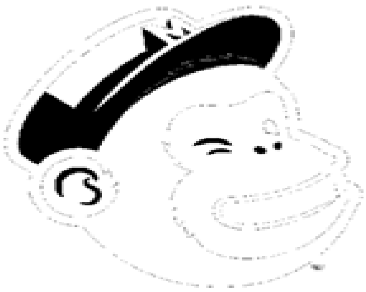
Bit plane 5



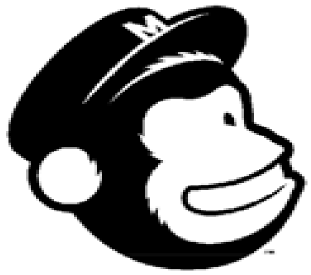
Bit plane 6



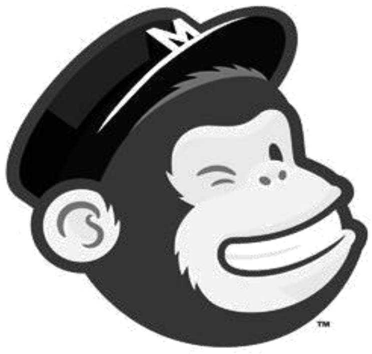
Bit plane 7



Bit plane 8



On overlapping the images, the final output image will be



Final image after decryption

9. RESULTS AND DISCUSSION

The proposed method introduces a bit slicing of grayscale image which in turn will be used in visual secrete sharing. Using this method, the quality of recovered image is increased without any noise. This technique provides two tier securities for grayscale images first by creating bitmaps and then creating shares for each bitmap. With this encryption and decryption process we can able to provide a strong method of security and are less likely to be hacked by hackers. This method will help in different areas and with standard application like MATLAB and Python this operation will be preferred.

10. REFERENCES:

[1.] *Nakajima, M., & Yamaguchi, Y. (2002). Extended visual cryptography for natural images*.

[2.] Kulkarni, P., & Kulkarni, G. (2018, March). Visual Cryptography based Grayscale Image Watermarking in DWT domain. In *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)* (pp. 1443-1446). IEEE.

[3.] Chen, T. H., Tsao, K. H., & Wei, K. C. (2008, November). Multiple-image encryption by rotating random grids. In *2008 Eighth International Conference on Intelligent Systems Design and Applications* (Vol. 3, pp. 252-256). IEEE.

[4.] Nakajima, M., & Yamaguchi, Y. (2002). Extended visual cryptography for natural images.

[5.] Chuman, T., Sirichotedumrong, W., & Kiya, H. (2018). Encryption-then-compression systems using grayscale-based image encryption for jpeg images. *IEEE Transactions on Information Forensics and Security*, *14*(6), 1515-1525.

[6.] Revenkar, P. S., Anjum, A., & Gandhare, W. Z. (2010). Survey of visual cryptography schemes. *International Journal of Security and Its Applications*, *4*(2), 49-56.

[7.] Lin, C. C., & Tsai, W. H. (2003). Visual cryptography for gray-level images by dithering techniques. *Pattern Recognition Letters*, *24*(1-3), 349-358.

[8.] Lukac, R., & Plataniotis, K. N. (2005). Bit-level based secret sharing for image encryption. *Pattern recognition*, *38*(5), 767-772.

[9.] Naor, M., & Shamir, A. (1994, May). Visual cryptography. In *Workshop on the Theory and Application of of Cryptographic Techniques* (pp. 1-12). Springer, Berlin, Heidelberg.

[10.] Kamboj, A., & Gupta, D. K. (2015, February). An improved Halftone Visual Secret Sharing Scheme for gray-level images based on error diffusion in forward and backward direction. In *2015 Fifth International Conference on Advanced Computing & Communication Technologies* (pp. 125-130). IEEE.

[11.] Al-Tamimi, A. G. T., & Gaafar, A. (2015). A New Simple Non-Expansion Algorithm for (2, 2)-Visual Secret Sharing Scheme. *International Journal of Computer Applications*, *113*(3).

[12.] Wu, Y. S., Thien, C. C., & Lin, J. C. (2004). Sharing and hiding secret images with size constraint. *Pattern Recognition*, *37*(7), 1377-1385.

[13.] Liu, S., Sun, J., & Xu, Z. (2009). An Improved Image Encryption Algorithm based on Chaotic System. *Jcp*, *4*(11), 1091-1100.

[14.] Verma, J., & Khemchandani, V. (2012). A visual cryptographic technique to secure image shares. *International Journal of Engineering Research and Applications (IJERA) ISSN*, *22489622*.

[15.] Hawkes, L., Yasinsac, A., & Cline, C. (2000). An application of visual cryptography to financial documents. *Florida State University, Florida*, 1-7.

[16.] Weir, J., Yan, W. and Kankanhalli, M.S., 2012. Image hatching for visual cryptography. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, *8*(2S), p.32.

[17.] Patel, T. and Srivastava, R., 2016, November. Hierarchical visual cryptography for grayscale image. In *2016 Online International Conference on Green Engineering and Technologies (IC-GET)* (pp. 1-4). IEEE.

[18.] Weir, J. and Yan, W., 2010. A comprehensive study of visual cryptography. In *Transactions on data hiding and multimedia security V* (pp. 70-105). Springer, Berlin, Heidelberg.

[19.] Katta, S., 2011. Visual secret sharing scheme using grayscale images. *arXiv preprint arXiv:1106.6242*.

[20.] Yu, Y.H., Chang, C.C. and Lin, I.C., 2007. A new steganographic method for colour and grayscale image hiding. *Computer Vision and Image Understanding*, *107*(3), pp.183-194.