Military Grid Reference System using Visual Cryptography

Shameema K[1], Sreekala R[2]

[1]M.Tech Scholar, Department of Computer Science and Engineering, Jawaharlal College of Engineering and Technology, Kerala, India
[2]Assistant Professor, Department of Computer Science and Engineering, Jawaharlal College of Engineering and Technology, Kerala, India

---***---

Abstract - *Data security is the process of protecting information and data systems from malicious access, use, disclosure, disruption, alteration or destruction. Visual cryptography encrypts the secret image into a visual image form by hiding the secret image with a cover image. Recent years, apart from the academic and institutional information security, Military information security is very important. In the system main focus is on applying Visual Cryptography on colour image. So Half tone method was used. The system give more importance to the date on which Visual Cryptography will be applied. The system to hide a secure data first steganography technique used will be based on Vedic Numeric Code in which coding is based on tongue position. In vedic numeric coding English alphabets are assigned for the vedic numbers to convert the secret numbers into alphabets. Then the stenographed image will be used as the input to the Visual Cryptography. The method enables more security provided to the data. By achieving the system it can also prove better Correlation, Universal Quality Index(UQI) and Structural Similarity(SSIM) factors.*

***Key Words*: Visual Cryptography, Encryption, Decryption, Vedic numeric coding, Halftoning.**

1. INTRODUCTION

Visual Cryptography is first proposed by Naor and Shamir in 1994. Visual cryptography is related to the secret holding mechanism which protects the secret data from unauthorized users. VC divides the secret image data into binary images into many shares and each shares alone cannot reveal any information about the data. Therefore only the user having complete shares can access the information. VC is the new era of methodology in the privacy security of the confidential data's including medical data, military codes, bank details etc. The shares of secret images are superimposed to get the original image data. Various methods are generated every year to give the accurate data after the VC operations. Main target of accepting various method is depended upon the handling of visual quality and security. Ordinary cryptography method uses public key, private keys etc. In case of visual cryptography the concept of key becomes secret image, target image, cover image etc. Here the key concepts are not used. Here, the paper describes about the military grid reference system. Here the area will be divided into many grids, and MGRS is used to specify these locations which is divided into different grids. Grids are divided as squares. When the image is converted into n shares in VC, at the end process of the process the n shares should be stacked completely to get the secret image. But in case of (k, n) method only k number of shares from total n shares can be joined to regenerate the secret image. In a (k, n) visual cryptography method at least k number of suitable shares should be used to get the secret image, where k≤n. the accurate data after the VC operations. Main target of accepting various method is depended upon the handling of visual quality and security. Ordinary cryptography method uses public key, private keys etc. In case of visual cryptography the concept of key becomes secret image, target image, cover image etc. Here the key concepts are not used. Here, the paper describes about the military grid reference system. Here the area will be divided into many grids, and MGRS is used to specify these locations which is divided into different grids. Grids are divided as squares. When the image is converted into n shares in VC, at the end process of the process the n shares should be stacked completely to get the secret image. But in case of (k, n) method only k number of shares from total n shares can be joined to regenerate the secret image. In a (k, n) visual cryptography method at least k number of suitable shares should be used to get the secret image, where k≤n. According to the (k, n) method the secret image is divided into n shares and only efficient k shares is required to recreate the secret image.

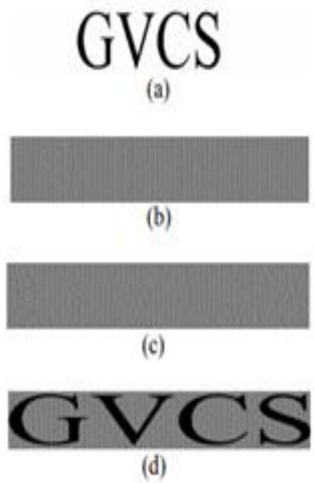


Fig.1.: Example (2, 2) visual cryptography

Here the secret image is divided into 2 and they are hidden with a cover image. Again these cover image is combined in the receiver side, then the original image is extracted from it. In a (k,n) visual cryptography a k number of shares from the complete shares are rejoined to get the original secret image. DBS, Vedic numeric coding, halftoning with error diffusion are the emerging methods in visual cryptography. DBS, Vedic numeric coding, halftoning with error diffusion are the emerging methods in visual cryptography. Another main method for the halftoning is error diffusion. The term error diffusion is the main master plan for the error diffusion. Because error diffusion filters the errors and distribute that errors by balancing their value. Therefore every pixel in the image will be carrying similar amount of errors, then the visibility of the image will be more natural. The emerging methods in cryptography is Honey pot method, Quantum key distribution etc.

2. LITERATURE SURVEY

A large amount of data is being transmitted and exchanged over the internet every day. However, it is noted that data transmitted over internet or stored in internet servers may be captured by the attackers if the data are not encrypted by good algorithms. Therefore, information security is one of the most important task in the field of modern computerized networks. Visual secret sharing (VSS) is one such scheme which can be used to handle the situation[1]. Visual Cryptography was developed by Noar and Shamir [1]. Halftone Visual Cryptography scheme produce halftone shares taking meaningful visual information which reduces the suspicion of intruders [1]. Halftoning is a representation technique to transform the original continuous tone digital image into a binary image consisting only of 1's and 0's.[9] According to the scheme, first of all a halftone image obtained by applying any halftoning technique such as the Floyd or Jarvis error diffusion algorithm[1]. .This is efficient algorithm for halftoning gray scale image. The quantization error at each pixel is filtered and fed back to a set of future input samples[9]. Fig.2. shows a binary error diffusion diagram where f(m, n)represents the (m, n) pixel of the input grayscale image, d(m, n) is the sum of the input pixel value and the diffused past errors, and g(m, n) is the output quantized pixel value[9]. Encryption process construct the meaningful shares using both input halftone image and halftone secret image by applying basic visual(2,2)scheme[9]. The information of secret image is encoded into halftone image I and inverse of halftone image I' .To encode a secret pixel p into a Q1xQ2 halftone cell in each of the two shares, only two pixels, referred to as the secret information pixels, in each halftone cell need to be modified. The two secret information pixels should be at the same positions in two shares. However, as long as their locations are independent of the secret information construction. It satisfies the security condition.

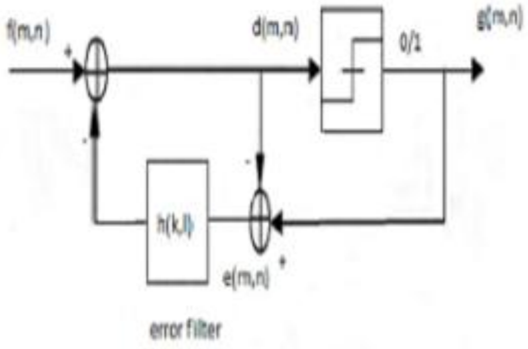


Fig.2. Error Diffusion block diagram

The simplest method to select the locations of the secret information pixels in halftone images is random selection [9]. Decryption Process the embedded secret is reconstructed from the shares. Shares obtained in phase 2 are stacked on each other. After the shares are superimposed, the meaningful information disappears and the secret is recovered [9]. Among many methods, the quality of the halftone image produced by DBS is the best and it has been extended to various printer models, different HVS models, color halftoning, screen design, and clustered dots [11]. The reason that DBS can generate halftone images of the best quality is that it seeks to minimize the total squared perceived error while algorithms in point and neighborhood processes are mostly heuristic. The search of a solution for DBS involves two operations: toggle and swap. The toggle operation finds one of the binary states for each pixel to minimize the squared error while the swap operation tries to switch two pixels of opposite states for the same purpose[11]. DBS tries to minimize the mean squares perceptually filtered error between the continuous-tone image and output halftone image, and it is the most computationally efficient as an iterative process. In addition to significantly better halftone quality, DBS has a more attracting aspect of high flexibility[20]. Color tagged secret sharing scheme shares a tag secrets in the shares and reconstructs the tag secret by folding them[17]. Secrets and the tagged secrets are halftoned resulting in the halftoned secret and tagged secret. Three color channels Red, Green and Blue channels are processed separately for the generation of shares[17]. Traditional schemes used OR operation for decoding the secret. Even though OR operation offered computation free decoding, the visual quality of the recovered image was poor. So to enhance the visual quality use of XOR operation for decoding were proposed by Ching-Nung Yang and Dao-ShunWang [14].

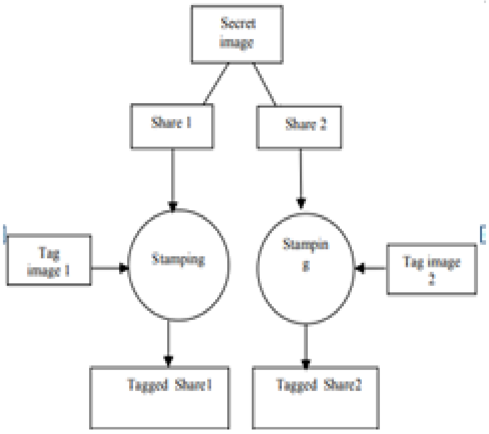


Fig.3. Tagged secret stamping process

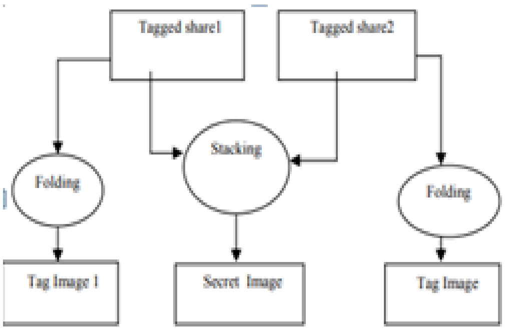


Fig.4. Tagged secret reconstruction process

Increased visually quality of cover images results in stronger security. In the paper these drawbacks are considered and two halftoning techniques Error Diffusion and Direct Binary Search(DBS) is implemented modified and compared for betterment. The method can be implemented for national security. Military Grid Reference System(MGRS) is taken has a reference but can be extended to any system which requires security[1].

3. METHODOLOGY

Military data sets are different types of codes which is not easy to read. Highly confidential data's about the security systems of the country and other important rout map details are transferred in each seconds by the military agencies. Therefore, security of the data is important at every time. Military data's including alphabetical codes are considered here including the digits also.

NORTHTWENTYFIVEMETERSANDSOUTHFI
FTYMETERSWITHASTRONGMUDAREABEHI
NDSUNDARBANSRIVER

Above military data is to be sent to the required agencies. Here the military grid reference system is taken as a reference also can be extended to other security systems. Before entering the visual cryptography stage, the grid code is to be hidden and converted to the form of an image. Above secret code is firstly converted to its corresponding Vedic numbers.

Vedic Numeric Coding

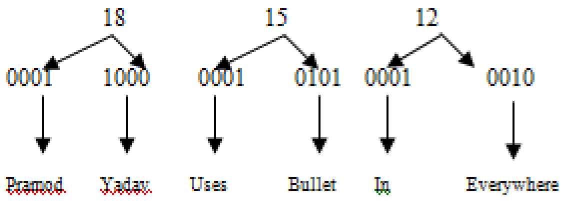
The code conversion into image is an ordinary method which can be easily attacked and read. Therefore, an intermediate step is added in between the text to image conversion. The text data is applied for a vedic numeric coding process and then it is converted to an image data. Vedic numeric coding is discovered from Indian history. Vedic numeric coding converts each letter or digit of the code into a vedic number. The conversion takes place after some continuous steps, which gives more security and will be difficult to attack the data.

```
55 58 78 95 81 95 71 54 95 76 63 90 91 54 45
54 95 54 78 93 12 55 46 93 58 92 95 81 63 90
63 95 76 45 54 95 54 78 93
……………………………………………………………………
…………………
```

Above table gives the corresponding values for each alphabets in the vedic numeric coding algorithm. In the next step the four bit binary values of each digits are taken as shown in the table below.

```
10111100 11100101 10101010 11111111
01010101 10110001 001000011 10101010
11111111 01010101 10101111 11001100
10101011101101111001000110010110111111
00010010011001100101001100110001100 11
00101011010101010110010010011110
```

Four bit binary values for each digit is pointed above. Then the alphabets for each binary number is taken and a meaningful sentence is written starting with the secret code letter. The next step for the process is converting each letter into a meaningful sentence as given below.



Visual cryptography

While entering into the visual cryptography stage, the data above is converted into an image form. In case of the form of data is only texts, the image format can be a grey scale image or a black and white image. Otherwise a coloured image should be converted into its corresponding range of colors in case of halftoning process. Military grid data will be in a grey type image.

Encryption

Visual cryptography require binary images to continue the different algorithms to work on the image. Therefore the secret image should be converted into different shares by using any of the methods including (2,2) to n share method, (k, n) share method. Here halftoning is using for the further operations on the image data. There are mainly two divisions in the types of halftoning, one is error diffusion and other one is DBS(Direct Binary Search) method, which is a searching algorithm to identify the exact matching for the perfect image. Here DBS is used for data processing. Because of the pixel comparisons taking place in DBS method, the secret image shares are converted into a halftoned image, which means that before applying any one of the process error diffusion or DBS the image should halftoned. Halftoning of the image converts the image into a combination of only black and white pixels. In case of colour images the pixels of the image will be included in any of the three groups including blue green and red also known as RGB colors. The figure below give the exact picture of a halftoned image. In case of DBS the secret shares are taken each one, and each pixels are toggled and swapped repeatedly. At each step of repetition it checks whether the toggled share is much clear than the early phase. The iteration is continued at a particular number of times. And at last the most improved share is taken to stack the image.

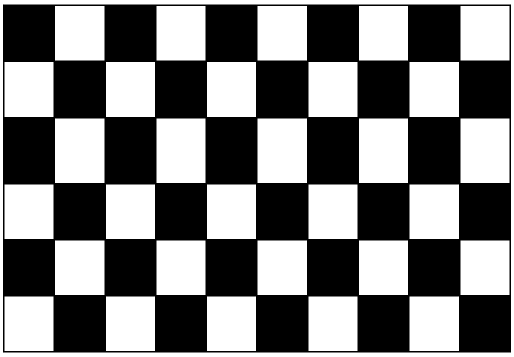


Fig .5. Halftoned image

After converting the image into a halftoned image pixel calculation will be easier. The image will be visually in the form of arrangement of visible pixels.

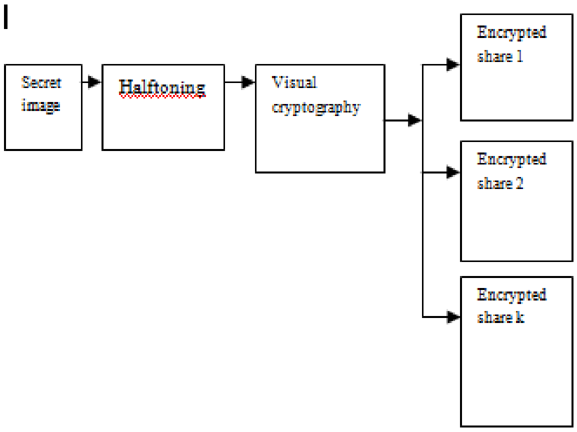


Fig.6.Encryption block diagram

(k, n) shares

In a (k, n) share method a secret image is obtained by combing k number of share images from a total of n images. But also the condition is to select only the required shares and combine them, then only the secret image will be revealed.

Decryption

Decryption is almost same in all visual cryptography. Because the shares generated by various methods are finally superimposed/stacked into an image in the stage of decryption. Here is the small representation of decryption process in the below figure.

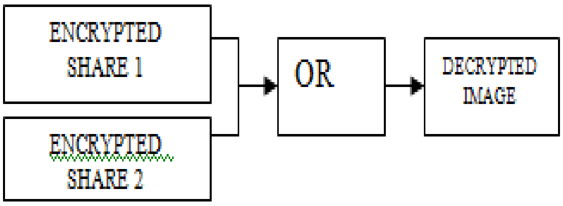


Fig.7. Decryption block diagram

Proposed method: Enhanced Direct Binary Search

Secret data is converted into an image form. and the image subjected to a halftoning process , now the image is converted as different shares. Now a handset of various shares of the image is in the box. Now the data is subjecting to ultra super algorithm known as Enhanced Direct Binary Search (EDBS). Direct Binary Search uses toggle and swap method. In case EDBS an optimal threshold method is also used along with the direct binary search. Detailed figure about the algorithm is given below.

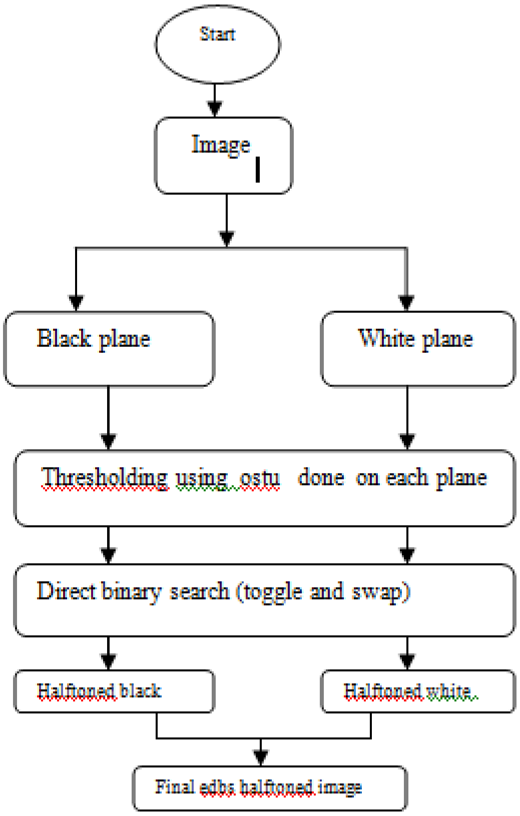

Start
Image
Black plane
White plane
Thresholding using ostu done on each plane
Direct binary search (toggle and swap)
Halftoned black
Halftoned white
Final edbs halftoned image

Fig. 8. Proposed method using EDBS

Black and white image is subject for sharing process and is converted as different shares. The shares are again classified into black plane and white plane according to the values assigned for the black and white colors. After that, thresholding is done using OSTU on each plane and again the black and white planes are classified more strictly by exact comparison. Then the shares are subjected to DBS process including toggle and swap techniques. Each shares are taken and examine the quality and improvement of the image after DBS process. At each step the result is obtained for each shares. Again after the DBS process the resultant share are divided into two components as halftoned black plane and halftoned white plane. And the two components are joined to get the final halftoned image.

4. CONCLUSIONS

Visual cryptography encrypts the secret image by converting it into different shares. For providing advanced security for the confidential data of the military agencies a wide range of algorithms is to be developed. But according to the modern generation skills any standard algorithm developed by the designers are hacked by the attackers. Therefore, to make them confused and to make a twist in the standard algorithms will help to set the data without an attack fear. Here the standard algorithm naming halftoning process is using after changing the total look of original data. Here the newly launched method named Vedic numeric coding is using to change the form of the data into another totally different appearance. Therefore when the attackers can attack the halftoned data, but the form of the data will not be understandable. The situation can provide more relaxation for the security providers in getting much time to safe the data. The standard algorithm halftoning includes two major steps naming error diffusion and direct binary searching. Enhanced direct binary search is the emerging function, which can give halftoning much accuracy.

REFERENCES

1. Sandhya Anne Thomas, Saylee Gharge(2018), Enhanced Security for military grid reference system using visual, *International Conference On Computing, Communication and Network Technologies, IEEE.*
2. Sandhya Anne Thomas(2018), Halftone Visual Cryptography For Grayscale Images Using Error Diffusion And Direct Binary Search, 2018 *2nd International Conference on Trends in Electronics and Informatics ,IEEE,*4,5386-3570.
3. LuLuo,PengCao,DazhongMu (2017),Research on High-Resolution Imaging Technology to Extract the Halftone-Dot-Information by iPhone, *International Conference on Intelligence and Security Informatics (ISI) IEEE,*5090-6727.
4. JitendraSaturwarD.N. Chaudhari (2017),Secure Visual Secret Sharing Scheme for Color Images Using Visual Cryptography and Digital Watermarking, Second *International Conference on Electrical, Computer and Communication Technologies ,IEEE,*5090-3239.
5. S.Sowmiya I.Monica Tresa A.Prabhu Chakkaravarthy (2017), Pixel Based Image Encryption Using Magic Square, *International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies, IEEE.*
6. R. M Shiny, P Jayalakshmi, A Rajakrishnammal (2016), An Efficient Tagged Visual Cryptography For Color, *International Conference on Computational Intelligence and Computing Research(ICICI), IEEE*, 978-5090.
7. Vandana Purushothaman, Sreela Sreedhar (2016), An improved secret sharing using XOR-based Visual Cryptography, *Online International Conference on Green Engineering and Technologies(IC-GET) , IEEE* ,978-5090.
8. Fuping Wang, Jan P. Allebach(2016), Printed Image Watermarking Using Direct Binary Search Halftoning, *International Conference on Image Processing, IEEE*, 4673-9961.
9. M.Desiha,Vishnu Kumar Kaliappan (2015), Enhanced Efficient Halftoning Technique used in Embedded Extended Visual Cryptography Strategy for Effective Processing , *International Conference on Computer Communication and Informatics , IEEE* , 4799-6805.
10. Akshara M. Gaikwad, Kavita R Singh (2015), Embedding QR Code in color images using Haftone Technique , *2nd*

International Conference on Innovations in Information Embedded and Communication Systems,IEEE,4799-6818.

11. Jan-Ray Liao, (2015), Theoretical Bounds of Direct Binary Search Halftoning,Transactions on Image Processing , *IEEE* , Vol 24,1057-7149.

12. Zifen He, Yinhui Zhang(2015), Watermarking Hiding in Halftoning Image, International Conference on *Intelligent Systems Research and Mechatronics Engineering, ISRME*,1390-1393.

13. Hsiang-Cheh Huang ; Feng-Cheng Chang(2015), Visual Cryptography for Compressed Sensing of Images with Transmission over Multiple Channels , *International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (IIH-MSP*), IEEE*,63-66.

14. Aman Kamboj ,D.K. Gupta (2015), An Improved Halftone Visual Secret Sharing Scheme for Gray-Level Images Based on Error Diffusion in Forward and Backward Direction, *Fifth International Conference on Advanced Computing & Communication Technologies, IEEE*,2327-0659.