International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-4, April 2019

Cheat Immune visual Cryptography for Secure Transmission of Images

Ranjan Kumar H S, Sampath Kini, Akshatha L, Deeksha B G

Abstract: ***Transmission of confidential information securely on insecure communication channel is atmost important. Image encryption is a method which is used to hide the secret image. During the course of transmission over insecure communication network, intruders may alter the encrypted data and may result in changing the visual meaning of the image. In this paper, a novel cheat immune image encryption technique is proposed. If a middle man tries to alter the encrypted data than decryption of an image fails. During encryption, it divides the source image into '3' shares and decrypts by superimposing all the 3 shares. In this technique, secret information or image can be retrieved only if all three shares are in possession. The traditional visual cryptographic scheme suffers from the problem of pixel expansion. In this aspect ratio of an image changes resulting in increasing the width of encrypted image. To overcome this, a novel random grid visual cryptography is proposed. The methodology uses Residue Number System (RNS) for encryption and utilizes Mixed Radix Representation(MRR) for decryption. RNS and Mixed radix is mainly used in fault tolerance. This is designed so as to avoid cheating during decryption.***

Index Terms**: Encryption, decryption, residue number system, mixed radix representation, pixel expansion.**

I. INTRODUCTION

The Internet is one of the widely used source of information and activities. It has become a major concern now for secrecy of data and to protect the copyright of data. To achieve these, many steganography techniques have been developed. But each one of them have their own pros (advantages) and cons (disadvantages). If one technique lacks in payload capacity, the other lacks in robustness. Visual cryptography is used to encrypt visual data to a format that will be very tedious for an intruder to crack it. In 1994, Naor et al. [1] developed a unique and well-known scheme.In this scheme, they divided a secret image into 'n' shares and if it needs to be decrypted then all the 'n' shares should be known by the entity decrypting it. Even if one of the shares is not known, then the secret image wouldn't be exposed. This means that the final image is produced only after stacking up all the n shares. k-out-of-n visual cryptography scheme is known to be one of the generalization of this scheme. Visual cryptography has its own applications. Majorly it could be used for biometric authentication. It could also be used to provide secured digital transmission.

Manuscript published on 30 April 2019.
***** Correspondence Author (s)
Ranjan Kumar H S*, Computer Science & Engineering, NMAM Institute of Technology, Karkala, India.
Sampath Kini, Computer Science & Engineering, NMAM Institute of Technology, Karkala, India
Akshatha L, Computer Science & Engineering, NMAM Institute of Technology, Mangalore, India.
Deeksha B G, Computer Science & Engineering, NMAM Institute of Technology, Mangalore, India.

II. LITERATURE SURVEY

This section describes the research work of some of the prominent researchers in visual cryptography and provides a short description of various techniques used for encryption and decryption. The state of art of image encryption techniques is classified as traditional key based cryptography and Visual cryptography.

A. Traditional key based image encryption

This section gives the brief insight on works carried by researchers based on traditional key based image encryption techniques.

Zhenjun tang et. al [2] proposed "Image Encryption with Double Spiral Scans and Chaotic Maps". In this, they proposed image encryption algorithm on the basis of chaotic maps and double spiral scan. The image is divided into various blocks and pixels of each blocks is responsible for scrambling through double spiral scan. At this point chaotic maps were selected randomly next image content is generated with help of secrete keys. These keys were used to control Lu chaotic map and also used for calculating secret matrix of the input image. At last encryption done by XOR operation between scrambled images and secret matrix of the input image. Akram belazi et. al [3] proposed "Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms". In this, they focused on image encryption technique with help of substitution boxes (S – boxes) which is used to generate chaotic systems and linear fractional transform (LFT). Here the encryption scheme is proposed with confusion and diffusion done by block permutation, substitution and diffusion. The S-boxes were constructed by adding chaotic map and LFT. The scheme is used to encrypt only requisite parts, the approximate coefficients in LWT frequency domain and sensitive information.

Ahmad Habibizad Navin et al. [4] proposed "A Novel Approach Cryptography by using Residue Number System". In this, they worked on residue numbers which is used to compress the information by encrypting Huffman coding and Lempel-ziv-welch (LZW) and to get the high security data encryption standard algorithm is used.

Guodong Ye et. al [5] proposed "A Chaotic Image Encryption Algorithm Based on Information Entropy". In this, based on information or data entropy of chaotic maps, image encryption scheme is proposed.

The method used for this scheme is PMD i.e permutation, modulation and diffusion. Data entropy employed with large key streams. Here the initial key used for permutation and diffusion methods. To provide high security for communication method in image PMD method is proposed with image encryption algorithm.

Saeed noshadian et. al [6] proposed "Optimizing chaos based image encryption". In this, they proposed image encryption technique to solve sensitivity issues in images. In the first step, image is applied for confusion method with help of logistic map to get chaos based function and diffusion is done by shuffling algorithm called as KNUTH shuffling algorithm. This algorithm is used to speed up the optimization technique which gives the lowest co-relation among highest entropy.

I. A. Ismail et al. [7] proposed "A Digital Image Encryption Algorithm Based a Composition of Two Chaotic Logistic Maps". In this, they have done image encryption with help of large external secret keys and chaos based cipher which adds two chaotic logistic maps which is used to mystify the association established encrypted image and secret image. With the encryption process they have focused on various features like high level of security, large enough key space and uniformity distribution of pixels.

B. Visual Cryptography

Visual cryptography is popularly known as 'Keyless image encryption' can be utilized to encrypt the visual data. The state of art of image encryption techniques proposes many algorithm which is concerned to provide security for visual data.

Roberto et al. [8] proposed "color visual cryptography schemes for black and white secret images". In this, they have proposed improved color version for visual cryptography schemes which is used for black and white secret images, to achieve this scheme "colored black and white visual cryptography model (CBW-VC)" is used. Usually in the black and white visual cryptography the secret images are black and white. To get improved version of visual cryptography colored images are used with black and white model to get best pixel expansion in "b&w model". They have also achieve achieved the contrast between the colors.

Mahmoud E et al. [9] proposed "An optimal (k, n) visual secret sharing scheme for information security". In this, they have focused on pixel expansion with help of new (k, n) scheme by code book and transposing of matrices. Without any distortion they have reconstructed secret image accurately. The disadvantage of secret sharing scheme is the size of the shared secret image is not reduced, and this process is done with help of XOR operation.

Aditya jain et al. [10] proposed "visual cryptography and image processing based approach for secure transactions in banking sector". In this, visual cryptography is based on XOR operation and image processing technique is used to secure transactions in banking section. The proposed method uses (2, 2) VCS XOR. Here the process is classified into two main phases i.e encryption and decryption phase. In the first phase two shares are generated, first share is called as BANK and second share is called as USER which is used by users. In the decryption process, when user wants to do transactions, bank performs the XOR operation between user shares and generated shares.

Ping Li et al. [11] proposed "A novel two-in-one image secret sharing scheme based on perfect black visual cryptography". In this, they have introduced secret image sharing method based on two decoding operation with help of two –in-one image secrete image sharing scheme. This scheme does not provide complex computation and also used in real time application. Here secret shares are obtained by adding grayscale secret image with Boolean operation then added to shadows of PBVCS (perfect black visual cryptography). This method is faster in decoding the secret image.

Yamini Ravella et al. [12] proposed "secret encryption using (2, 2) visual cryptography scheme with DCT compression". In this, they have provided solution to image security with help of visual cryptography and compression technique. Here cosine transformation technique is used. i.e DCT compression and IDCT decompression. These techniques are well performed on color and gray image. They have achieved good correlation between pixels as well as compaction properties and implementations are very fast.

III. PRELIMINARIES

A. Residue Number System

The basics of Residue Number System (RNS) reside in the theory of congruency. A pair x and y is congruent modulo n denoted by $x \equiv y \ (mod\ n)$, if the difference of x and y is integer multiple of n. Consider an example: $18 \equiv 2 \ (mod\ 4)$, *we get 18-2 = 16 which is integer multiple of 4.* Assume q and r as quotient and remainder of dividing an integer x by n i.e. $x = q \times m + r$, then we can also write it as $x \equiv$ r (mod n). Here r can be considered as residue of x and is denoted as $|x|_m$ *.Assume a list of positive integer's* $m_1, m_2 \ldots m_k$ *which are relatively prime. Given* $M = \prod_{i=1}^{k} m_i$ *, Any positive integer can be uniquely represented by its residues* $<x_1, x_2 \ldots x_k>$*, i.e.* $x_i = /x/_{mi}$ where i ranges from 1 to k. The dynamic range of x ranges from 0 to M. Consider an example, m_1=3, m_2=5, m3=7 where M=105, given x= 98 and its tuples are <2, 3, 0>.

B. Additive inverse

Additive inverse (AI) is a special property of arithmetic operation in number system. The rule says 'There is a number denoted by (–x) for every real number x'. When these x and (-x) are added together, the result is always a zero'. Symbolically we can represent AI as below

$$x \oplus_m (-x) = 0$$

Since m is always congruent to zero, we can rewrite the above equation as

$$x + (-x) = m$$

or

$$(-x) = m - x$$

Consider for example the additive inverse of 8 and m is 12, Therefore –x = 12-8 = 4.The property of AI is utilized to represent negative numbers in RNS.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

C. Multiplicative inverse

Every non-zero real number *x* has a multiplicative inverse *I* if and only if the Greatest Common Divisor (GCD) of modulus *m* and *x* is equal to zero. That is

$$x \otimes_m I = 1$$

This concept of multiplicative inverse is needed for reverse residue conversion.

D. Number Systems

The number systems which are most familiar can be Binary number system and Decimal number system. The former can be represented in the following form:

$$x = \sum_{j=0}^{n-1} Z_j \times 2^j$$

Likewise, the decimal number system can be represented as:

$$x = \sum_{j=0}^{n-1} Z_j \times 10^j$$

In general a number system can be represented as:

$$x = \sum_{j=0}^{n-1} Z_j \times p^j$$

Where *x* is the number z_j is set of permissible digits and p^j represents successive power of the same number called the weight of the corresponding digit position.

Example

134 in decimal number system have the form

$$134 = 1 \times 10^2 + 3 \times 10^1 + 4 \times 10^0$$

here we see that z_j values for different digit positions are 1, 3 and 4 which are associated with weights 10^2, 10^1 and 10^0 respectively. Therefore, the base of decimal number system is 10. From the above example of the Decimal Number System, we also observe that it has the positional characteristics along with weight. The digits- 1, 3 and 4's positions are fixed with their weights.

i. Mixed Radix Number System

Mixed Radix Number System (MRNS) is another way of representing a number, where in the base of each digit of a number varies, hence the name "Mixed Radix". Consider for example, a method for representing 604800 seconds in a week, where in 0-6 represents days of week, 0-23 represents hour of a day, 0-59 represents minute of an hour and 0-59 represents second of a minute. The MRNS may be used to represent each second, for instance $4_7 18_{24} 23_{60} 18_{60,}$ is equivalent to 18:23:18 on Wednesday. The Mixed-Radix Conversion (MRC) achieves an association between the unweighted, non-positional RNS and a weighted, positional mixed-radix system.

E. Encryption by Residue Number System

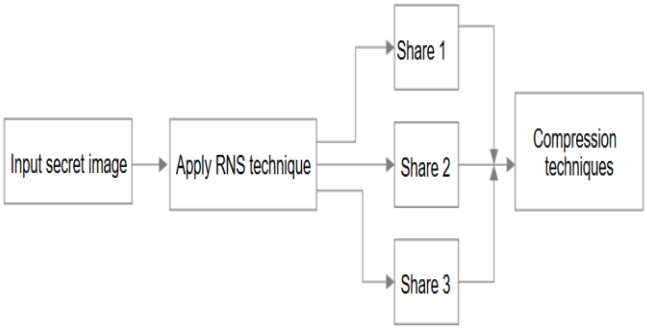

Fig. 1 Encryption block diagram

The block diagram for encryption process is as shown in fig.1. It utilizes the concept of RNS described in III.A. In this process, each pixel of an image and moduli set is taken as input. moduli set and then encrypt using the given moduli set and then find the residues. Encryption step includes:

S1[i]←X[i]%M1
S2[i]←X[i]%M2
S3[i]←X[i]%M3

where, A[5000] is the secret image and S1,S2,S3 are the 3 shares required to decrypt and get back original image. Moduli set is {M1,M2,M3}.

F. Decryption by mixed radix conversion

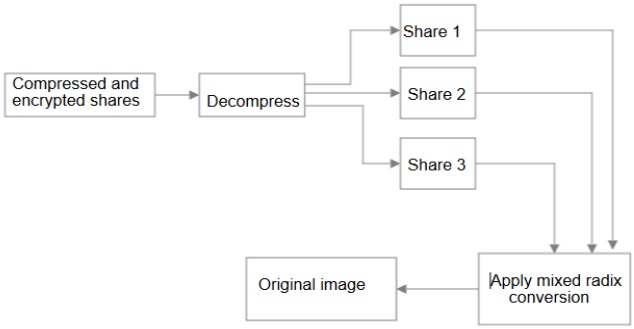

Fig. 2. Decryption block diagram

The block diagram for encryption process is as shown in fig.2.The input for decryption is S1,S2,S3 and modulii set{M1,M2,M3}. Output is the decrypted original image which is obtained using the following sequence of steps:

If the radices are r_N, r_{N-1},..... r_1, any number X in mixed-radix form can be given as: X $\cong$ (c_N , c_{N-1} , c_{N-2},.....c_1) .

which means

$$X = c_N r_{N-1} r_{N-2} \ldots r_1 + \cdots + c_3 r_2 r_1 + c_2 r_1 + c_1$$

where $0 \leq c_i < r_i$.

This means that it is a weighted, positional number system. The conversion from RNS to a mixed-radix number is called a reverse transform.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Next we need to identify c_i and find on how to convert it to X.

Using (a_N , a_{N-1} , ..., a_1) with respect to moduli $b_1, b_2, \dots, b_N$, we make the $a_i s$ correspond to the $b_i s$. That equation then becomes:

$X = c_N b_{N-1} b_{N-2} \dots b_1 + \cdots + c_3 b_2 b_1 + c_2 b_1 + c_1$ (1)

i. Identify c_1

Taking modulo with respect to b1, on both sides of this equation:

$|X|_{b1} = c_1$

$= a_1$

Therefore,

$\mathbf{c_1 = a_1}$

ii. Identify c_2

Equation (1) can be written as:

$X - c_1 = c_N b_{N-1} b_{N-2} \dots b_1 + \cdots + c_3 b_2 b_1 + c_2 b_1$

Taking modulo with respect to b_2 :

$|X - c_1|_{b2} = |c_2 b_1|_{b2}$

Multiplying both sides by $|b_1^{-1}|_{b2}$ yields:

$\big| |b_1^{-1}|_{b2} (X - c_1) \big|_{b2} = |c_2|_{b2}$

$= c_2$ (since $c_2 < b_2$)

Also,

$|X - c_1|_{b2} = \big| |X|_{b2} - |c_1|_{b2} \big|_{b2}$

$= |a_2 - c_1|_{b2}$ (since $c_1 < b_2$)

Therefore,

$$\boldsymbol{c2 = \big| |b_1^{-1}|_{b2} (a_2 - c_1) \big|_{b2}}$$

iii. Identify c_3

Equation (1) can be written as:

$X - (c_2 b_1 + c_1) = c b_{N-1} b_{N-2} \dots b_1 + \cdots + c_3 b_2 b_1$

Taking modulo with respect to b_3 :

$|X - (c_2 b_1 + c_1)|_{b3} = |c_3 b_2 b_1|_{b3}$

Multiplying both sides by $|(b_2 b_1)^{-1}|_{b3}$ yields:

$\big| |(b_2 b_1)^{-1}|_{b3} (X - (c_2 b_1 + c_1)) \big|_{b3}$

Also,

$|X - (c_2 b_1 + c_1)|_{b3} = |X|_{b3} - |(c_2 b_1 + c_1)|_{b3}$

$= | a_3 - (c_2 b_1 + c_1)|_{b3}$

Therefore,

$$\boldsymbol{c_3 = \big| |(b_2 b_1)^{-1}|_{b3} (a_3 - (c_2 b_1 + c_1)) \big|_{b3}}$$

Here $a_1, a_2, \dots, a_n$ is the residue set.

$b_1, b_2, \dots, b_n$ is the moduli set.

Example: Let's assume, the number (or pixel value) to be encrypted (X) is198.

Assume that the moduli set = {5, 7, 11}

Encryption

Finding residue representation of X:

$a_1 = 198 \% 5 = 3$

$a_2 = 198 \% 7 = 2$

$a_3 = 198 \% 11 = 0$

Therefore, 198 (X) is encrypted as tuple <3, 2, 0>

Decryption

$X = c_3 b_2 b_1 + c_2 b_1 + c_1$ (2)

To find c_1

$c_1 = a_1$ => $c_1 = 3$

To find c_2

$$c_2 = \big| |b_1^{-1}|_{b2} (a_2 - c_1) \big|_{b2}$$

$$c_2 = \big| |5^{-1}|_7 (2 - 3) \big|_7 \quad (3)$$

$5^{-1} \bmod 7$ => Let x = 5 ; y=7

Now, x = x % y = 5 % 7

=> x = 5 ; y=7

Find an 'a' such that, (x × a) % y =1

We can see that a = 3

Therefore, $5^{-1} \bmod 7 = 3$

Now in (3),

$c_2 = \big| 3 (2 - 3) \big|_7 = \big| -3 \big|_7$

To find c_2,

Let, a = -3 ; b = 7

Let, temp = (a % b) + b

= (-3 % 7) + 7

temp = 4 + 7 = 11

temp = temp % b

= 11 % 7 = 4

⇨ $c_2 = 4$

To find c_3

$c_3 = \big| |(b_2 b_1)^{-1}|_{b3} (a_3 - (c_2 b_1 + c_1)) \big|_{b3}$

$c_3 = \big| |(7 \times 5)^{-1}|_{11} (0 - (4 \times 5 + 3)) \big|_{11}$

$c_3 = \big| |35^{-1}|_{11} (0 - (20 + 3)) \big|_{11}$

$c_3 = \big| |35^{-1}|_{11} (-23) \big|_{11}$ (4)

Now, $35^{-1} \bmod 11$, Let x = 35; y = 11

i.e. X = X% y = 35 % 11 = 2

X = 35; y = 11

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

find an 'a' such that,

$$(X \times a) \% y = 1$$
$$(2 \times a) \% 11 = 1$$

We can see that a = 6
Therefore, $35^{-1} \bmod 11 = 6$

Now in (4),

$c_3 = |6(-23)|_{11} = |-138|_{11}$
c_3 = -138 mod 11

To find c_3,

Let, a = -138; b = 11 and
Let, temp = (a % b) + b
= (-138 % 11) + 11
temp = 5 + 11 = 16
temp = temp % b
= 16 % 11 = 5
⇨ c_3 = 5

Now, in (2)

$X = c_3b_2b_1 + c_2b_1 + c_1$
$= 5\times7\times5 + 4\times5 + 3$
$= 198$

IV. EXPERIMENTAL RESULTS & ANALYSIS

At first, an authenticated user must select the image that needs to be encrypted. Next we need to read the selected image and encryption needs to be performed with the help of Residue Number System. Once the encryption process is completed, three shares will be generated. With the help of these shares and using mixed radix conversion for decryption process, original secret image can be retrieved.

The proposed technique is implemented using Java tool. We take lena.bmp image as the input image for experimental analysis.

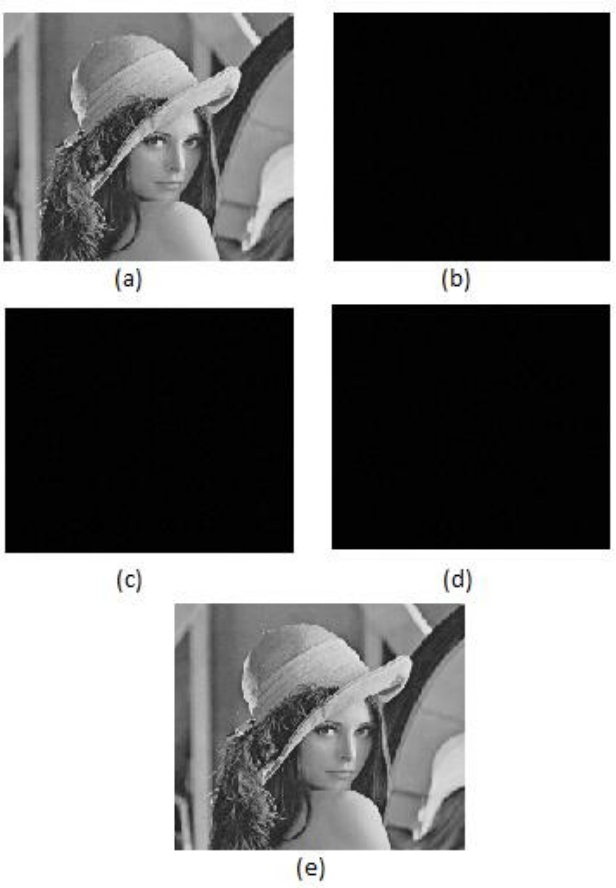

Fig. 3. (a) Input image. (b) share1. (c) share2. (d) share3. (e) decrypted image.

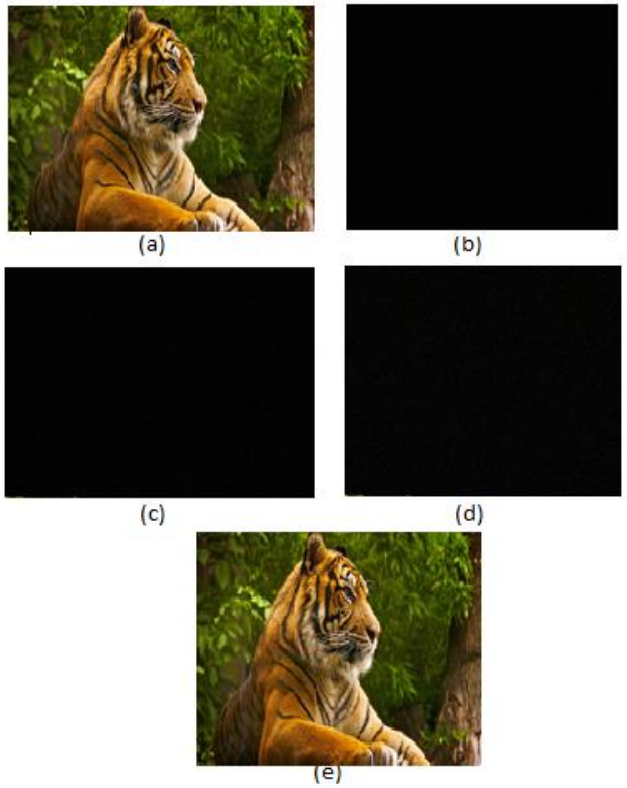

Fig. 4 (a) Input image. (b) share1. (c) share2. (d) share3. (e) decrypted image.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

A. Pixel expansion

Table 1: No of Pixels before and after encryption

Image	Length of image before encryption	Length of image after decryption
lena.bmp	263222	263222
tiger.bmp	669822	669822
girlface.bmp	263224	263224

From the above table, length of image after encryption and decryption has remained the same. It is evident that during encryption process, each pixel will get replaced by exactly one pixel. Hence there's no pixel expansion in the proposed method. Also by doing visual analysis the aspect ratio of encrypted image remains same. we can conclude that the proposed method is typical form of random grid visual cryptography.

B. Cheat Immune

The technique used for encryption is cheat immune and is evident from fig.5.The share2 of lena.bmp is altered and is used to decrypt the data. Since the share2 is not genuine decrypting the image into meaningful content fails as it is shown in fig 5. So decryption entity shows the noisy image when an intruder or a cheater tries to decrypt image using fake shares.

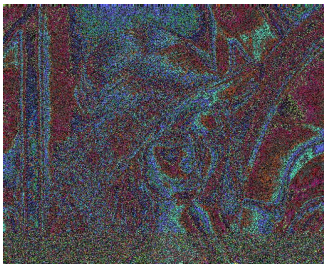

Fig. 5. Decrypting Lena image to random image since share2 is changed

C. Lossless Decryption

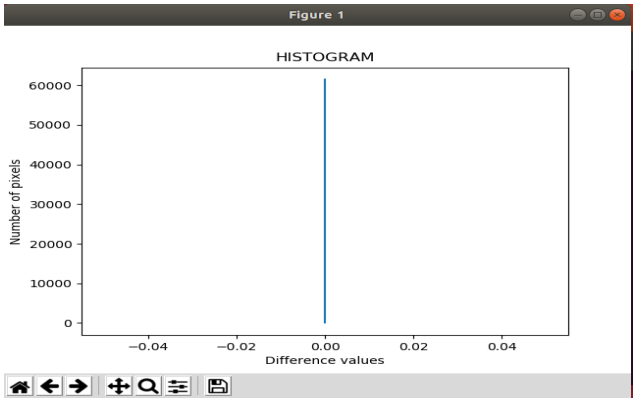

Fig. 6.Histogram of image obtained by subtracting pixels of original image with decrypted image.

The above histogram infers that there is no loss of data while decrypting the image. We take pixel values of both the images selecting one pixel at a time, and then we subtract the pixel values which results in zero.

D. n out of n cryptography

All the shares generated are required in order to decrypt the original image.

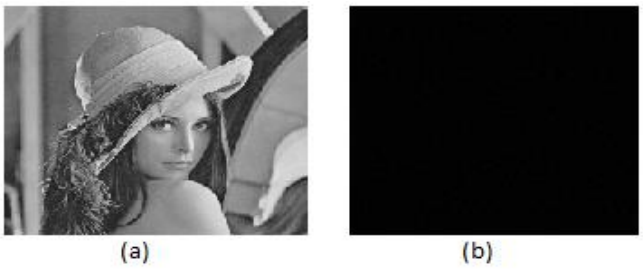

Fig. 7 n out of n cryptography

Fig. 7 shows us the decryption by selecting 'k' shares out of 'n' shares where k < n. We can observe that the decrypted image is not similar to the original image. Therefore our proposed work needs all 'n' shares in order to decrypt the original image.

V. CONCLUSION

Transmission of digital information securely on communication channel is atmost important. By 2025, approximately 75 billion people may connect to the internet. Due to this growth in the Internet usage, there may be a lot of possibility in hijacking the information. Information needs to be protected in ATM machines, Smartcards, E-commerce sites, etc. Security in these areas means preventing the information from getting into the wrong hands. Usually the databases have a lot of security issues and concerns.

The proposed visual cryptography technique used the mathematical relationship between RNS and Mixed Radix Representation. The technique used is Random Grid Visual Cryptography which don't involve any pixel expansion and aspect ratio of encrypted image is not changed. We also analyzed the decryption function and found that there is no loss in the image decrypted. The proposed method is n out of n Visual cryptography which needs all shares to decrypt the image. A secret information may be hacked only if it is easy to read and easy to understand. Intruders may expose, modify or use it to make an attack on other people or groups. The technique proposed is cheat immune i.e., if an intruder modifies the data than decryption fails.

REFERENCES

1. M. Naor and A. Shamir, "Visual Cryptography," in Proceedings of Advances in Cryptology-EUROCRYPT 94, LNCS 950, pp. 1-12, 1994.
2. Zhenjun Tang, Ye Yang, Shijie Xu, Chunqiang Yu, and Xianquan Zhang, "Image Encryption with Double Spiral Scans and Chaotic Maps," In Security and Communication Networks, vol. 2019,Jan 2019, pp.1-15.
3. Akram Belazi, Ahmed A. Abd El-Latif, Adrian-Viorel Diaconu, Rhouma Rhouma, Safya Belghith, "Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms" In Optics and Lasers in Engineering, vol. 88, 2017, pp. 37-50,

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

4. A. H. Navin, A. S. Khashandarag, A. R. Oskuei and M. Mirnia, "A novel approach cryptography by using Residue Number System," 6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), Seogwipo, 2011, pp. 636-639.
5. Guodong YeChen Pan, Xiaoling Huang, Zhenyu Zhao and Jianqing He "A Chaotic Image Encryption Algorithm Based on Information Entropy" In International Journal of Bifurcation and Chaos, Vol. 28, No. 1,2018, pp.1-11.
6. Noshadian, S., Ebrahimzade, A. and Kazemitabar,"Optimizing chaos based image encryption" In Multimedia tools and applications,vol.17,No.19, pp 25569–25590, Feb 2018.
7. Ismail Amr Ismail and Mohammed Amin and Hossam Diab "A Digital Image Encryption Algorithm Based A Composition of Two Chaotic Logistic Maps" In International Journal of Network Security,Vol.11,pp.1-10,2010.
8. Roberto De Prisco, Alfredo De Santis, "Color visual cryptography schemes for black and white secret images" In Theoretical Computer Science,Vol.510,pp.62-86,2013
9. Mahmoud E. Hodeish, Linas Bukauskas, Vikas T. Humbe, "An Optimal (k,n)Visual Secret Sharing Scheme for Information Security",Procedia Computer Science, Volume 93, 2016, pp.760-767.
10. A. Jain and S. Soni, "Visual cryptography and image processing based approach for secure transactions in banking sector," 2nd International Conference on Telecommunication and Networks (TEL-NET), Noida, 2017, pp. 1-5.
11. Li, P., Yang, CN. & Kong ," A novel two-in-one image secret sharing scheme based on perfect black visual cryptography" In Journal of Real-Time Image Processing,vol.14,No.1,2016,pp.41-50.
12. Y. Ravella and P. Chavan, "Secret encryption using (2, 2) visual cryptography scheme with DCT compression," International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, 2017, pp. 344-349.

AUTHORS PROFILE

Ranjan Kumar H S, working as Assistant Professor in the Department of CSE, NMAM Institute of Technology, Nitte. He has 10 years of teaching experience and 2 years of research experience. He has published 9 research papers in reputed journals. He has also presented 6 conference papers in national & international conferences. He has received best paper award for the paper titled 'Enhanced Visual Cryptography using Mixed Key Generation and Symmetric key Encryption' in International Conference of Emerging Trends and Engineering during 2013.He is also recipient of Young achiever-2019 award from Institute for Exploring Advances in Engineering (IEAE).

Sampath Kini, working as Assistant Professor in the Department of CSE, NMAM Institute of Technology, Nitte. He has 10 years of industry experience and 9 years of teaching experience. He has published 3 research papers in reputed journals. He has also presented 5 conference papers in national & international conferences. He achieved customer satisfaction of more than 4 point out of 5. He is responsible for Interfacing with the customers for understanding customer priorities & requirements and Software delivery status/progress

Deeksha B G, Undergraduate in Bachelor of Computer Science and Engineering, NMAM Institute of Technology, Nitte -574110, Karnataka, India, Internship in networking R & S, Zonal level winner in Cisco networking, Hands – on workshop on gaming, Member of B G Educational and Charitable trust.

Akshatha L, Undergraduate in Bachelor of Computer Science and Engineering, NMAM Institute of Technology, Nitte -574110, Karnataka, India, Internship in networking R & S, Zonal level winner in Cisco networking.