https://dx.doi.org/10.24001/ijaems.3.8.1 *ISSN: 2454-1311*

A Modified Binary Encryption Algorithm based on Diffuse Representation

Dr. S. Radhakrishnan[1], R. Arthy[2], M. Sivasankari[3], B. Jegajothi[4], Dr. M. Mohamed Sathik[5]

[1,2,3,4]Department of Information Technology, Kamaraj College of Engineering and Technology, Virudhunagar, India
[5]Pricipal, Sathakathulla Appa College, Tirunelveli, India

Abstract**—** *In the era of Internet, the multimedia data can be used by anyone. There is a chance that unintended users get access to the data so, encryption is needed to hide the multimedia data from the unauthorized users. This paper proposes a modified binary encryption algorithm based on diffuse representation. Here a binary image is XORed with a random matrix and is divided into more number of non-overlapping sub-images. The modified encryption algorithm will produce an encrypted image with ¼th of dimension and increased number of bits. The proposed encryption algorithm is a symmetric encryption algorithm. The number of keys generated is equal to the number of non-overlapping sub-images. The key shall be transmitted by a private key encryption algorithm. The encryption of the key is not of interest in this paper. The proposed algorithm has high performance that it gives BER as 0% and infinite PSNR. Even grayscale images can be encrypted using this algorithm considering each bit-plane as a binary image.*

Keywords— BER, Encryption, Private Key Encryption, PSNR, Symmetric Encryption.

I. INTRODUCTION

Internet is accessible by anyone in the world. When a multimedia data is shared through the internet there is a danger of unintended users getting access to it. To avoid this encryption is used. The visual cryptography technique is to support the encryption process where the secret information is converted into a unreadable form [2]. Encryption is a method in which the meaningful data is transformed into meaningless data and is sent through the internet. To get access to the data one should do the reverse process called the decryption to get the data in the original form.

Encryption is originally done for the text data where the transformed content is not understandable. Encryption algorithms are divided into two major categories: Symmetric and asymmetric encryption. In symmetric encryption, the key that is used for encryption and decryption are same. But in the asymmetric encryption, the key used during encryption differs from that used during decryption.

The key that is used during the cryptographic process can be categorized into various types. The symmetric encryption uses secret key that is shared between sender and receiver for encryption and decryption. The asymmetric encryption uses (private key, public key) pair to perform the cryptographic operations. The key pair is generated by the user and the public key is made available to anyone. The sender encrypts the message using private key of their own and receiver decrypts the encrypted message using sender's public key which is available in public.

The various visual cryptographic schemes are mentioned in [6], [10] for binary image, gray-colored images. [4] address the Extended Hamming Code to generate key for encryption and decryption through which the code is self-correcting. A new symmetric key cryptographic algorithm is proposed in [5] where the algorithm withstands the security. A lossless and reversible encryption algorithm was introduced in [1] to address the pixel oversaturation by embedding the secret data into the several least significant bit planes of cipher text pixels by wet paper coding.

The algorithm [7] presents the probabilistics model which adopts the (t, n) visual cryptography scheme. This model efficiently manages the dynamically changing user group. The security level is improved using the bit level permutation technique in [8] for chaos based image ciphers. This technique proves better performance because the bits are shuffled between different bit planes.

The error diffusion method [9] is used to provide the solution for management problem. This method adds a cover image to each share to make the share visible. The error diffusion method is also used for shadow images [11]. This improves the quality of shadow image when compared to the existing algorithms.

The proposed algorithm in this paper is a symmetric encryption algorithm for binary images. The key used in symmetric encryption algorithm should not be disclosed publicly. The work in the paper is inspired from [3] which

https://dx.doi.org/10.24001/ijaems.3.8.1 *ISSN: 2454-1311*

uses a diffuse representation for encryption. A similar method is used to encrypt the binary image. However, the encryption algorithm used to encrypt the random matrix and the key is not the intent of this paper. Any asymmetric encryption algorithm may be used.

The rest of the paper is organized in the following manner. Section II discusses the existing algorithm from which this paper has been developed. Section III discusses the proposed algorithm of encryption and decryption. Section IV discusses some theoretical aspects by which the security in the algorithm can be increased. Section V discusses about the experimental results and Section VI gives the conclusion of the paper.

II. EXISTING ALGORITHM

A novel binary encryption algorithm based on diffuse representation is been proposed by Houas et al. In this paper a binary image has been taken and encryption algorithm is applied. The encryption algorithm can be described as follows:

2.1 Encryption

(a) A binary image (I) is taken

(b) Divide the image into n non-overlapping sub-images (I1, I2) each sub-image is taken to the size of the full image with the remaining partitions of a sub-image as zeros. Let it be called a share.

(c) The key for encryption β is calculated from all the shares by using the equation (1)

$$\beta(i,j) = \frac{1}{2}\left[\left(a_1(i,j) + \frac{||I_1||_1}{\sqrt{64}}\right) + \left(a_2(i,j) + \frac{||I_2||_1}{\sqrt{64}}\right)\right] \quad (1)$$

(d) The encrypted shares are formed from the key and the share by the equation (2) and (3)

$$b = \beta(i,j) - a_1(i,j) \quad (2)$$

$$b = \beta(i,j) - a_1(i,j) \quad (3)$$

The encrypted shares are formed by subtracting the share from the key. Knowing the key β, the random matrix and the encrypted shares the decryption can be done with the following decryption algorithm.

2.2 Decryption Algorithm

(a) The encrypted shares are taken

(b) The key β is taken

(c) All the encrypted shares are subtracted from the key and added together to from the decrypted binary image

Here a single key is used and the number of encrypted shares denotes the numbers of subimages. So once the key is hacked, then the image can be easily decrypted. To overcome this disadvantage the modified encryption algorithm based on diffuse representation is proposed. The proposed algorithm is discussed in section III.

III. PROPOSED ALGORITHM

The possibility of the hacker decrypting the encrypted image can be reduced by applying the proposed modified encryption algorithm.

Algorithm 1:

[Ien, Irm, Ikey] = Encryption [Im]

/* Notation: Im – Binary Image, Irm – Random Matrix, Ixor – Resultant Image after XOR, Idec – Share with Decimal values, Ikey – Key, Iencrypt – Encrypted Image Shares, Ien – Encrypted Image

*/

1. Read the Binary image (Im)
2. Generate a random matrix (Irm) of size equal to the Im
3. Ixor = Irm XOR Im
4. Divide the Ixor into 8 shares

// Perform for 8 shares

5. For i = 1 to row(Ixor) incr 2
   For j = 1 to column(share) incr 2
   Idec[i, j] = decimal_conversion(Ixor)
   Endfor
   Endfor
6. Calculate Ikey
7. Iencrypt = Ikey – Idec
8. Concatenate all the encrypted shares to obtain Ien

Fig. 1 – Proposed Encryption Algorithm

The Fig. 1 shows the encryption algorithm in detail. The input image is read as the binary image and a random matrix is generated to perform XOR operation. This converts the image matrix into a random matrix. The matrix is scanned from left to right and top to bottom by taking a 2 x 2 sized matrix each time and converted into a decimal numbers. The resultant matrix is of m/2 x n/2 sized matrix of decimal numbers.

The key for each non overlapping matrix (share) is calculated using the equation (4)

$$B_k = \frac{4||I_k||_1}{\sqrt{size}} \quad (4)$$

The Ikey is used to encrypt the shares and finally all the shares are concatenated to obtain the encrypted image.

The decryption process is the reverse of the encryption algorithm. The random matrix and keys are shared with the end user. The share of keys are not a part of this paper. The decryption algorithm is stated in the Fig 2.

https://dx.doi.org/10.24001/ijaems.3.8.1 *ISSN: 2454-1311*

Algorithm 2:
[Idecrypt] = Decryption [Ien, Irm, Ikey]

/* Notation: Irm – Random Matrix, Idec' – Share with Decimal values, Ikey – Key, Ien – Encrypted Image, Ien – Encrypted Image, Ibin - Share with Binary values, Idbin - Binary Decrypted Image, Idecrypt - Decrypted Image */

1.Read the Encrypted image (Ien)
2. Divide the Ien into 8 shares
// Perform for 8 shares
3. Idec' = Ikey - share
4. For i = 1 to row(Idec')
For j = 1 to column(share)
Ibin = binary_conversion(Idec')
Endfor
Endfor
5. Concatenate all the decrypted Ibin's to obtain Idbin
6. Idecrypt = Idbin XOR Irm

Fig.2 - Proposed Decryption Algorithm

IV. THEORETICAL ASPECTS

4.1 Random matrix

The hacker when hacks the encrypted image can easily view the original image. To avoid this situation a random matrix is generated to increase the security level in encryption. The matrix is a formed with 0's and 1's and then XORed with the original image.

4.2 Number of Keys

The proposed algorithm uses the symmetric encryption algorithm which takes the secret key for encryption and decryption. As per the theory of cryptography, the security increases when the size and number of keys increases. The proposed algorithm has 8 keys for 8 different shares that makes the hacker feel difficult to hack the key and identify the respective key for each share. Since, the secret key has to be shared among the users it has to be secured using private key cryptosystem.

4.3 Joining all the shares and shares of variable sizes

The encrypted image is a combination of all shares. The shares can be decrypted with the respective keys. If the keys are not in the order then it is not feasible to decrypt the image. The keys can be send to the receiver by shuffling and encrypting which may be baffle the hacker to rearrange the key. There are (8! - 1) ways to shuffle the key.

4.4 Mapping of the 2 x 2 pixel matrix to a decimal number

The 16! ways of mapping 0000 – 1111 binary to decimal 1 – 16. One such mapping is as follows

0000 - 15	0100 - 11	1000 - 7	1100 - 3
0001 - 14	0101 - 10	1001 - 6	1101 - 2
0010 - 13	0110 - 9	1010 - 5	1110 - 1
0011 - 12	0111 - 8	1011 - 4	1111 - 0

A random mapping can be used so that the mapping may not be deciphered by the hacker. These are some of the methods by which security has been added to encryption algorithm.

V. EXPERIMENTAL RESULTS

The proposed algorithm is tested with the standard images like lena, cameraman, Barbara, baboon and Peppers. These image are converted into binary images and taken as test images. The binary images (I1) are encrypted and then decrypted (I2) using the proposed algorithm. The performance of the algorithm is calculated by using the metrics like Bit Error Rate (BER) and Peek Signal to Noise Ration (PSNR).

The PSNR is Peak Signal to Noise Ratio is an error comparison metrics to ensure that the decrypted image looks similar to the encrypted image. The PSNR value is calculated using the formula mentioned in equation (5) and (6).

$$\mathbf{PSNR} = \mathbf{10\log_{10}(L\text{^}2/MSE)} \quad (5)$$

$$MSE = \sum\sum \frac{(original - extracted)^2}{H * W} \quad (6)$$

Where,

L - Maximum fluctuation of input image
H - Height of the object
W - Width of the object

The Bit Error Ratio (BER) is the number of bit errors divided by the total number of transferred bits during a studied time interval. The equation (7) shows the calculation of BER value.

$$BER = \frac{Number\ of\ pixel\ wrongly\ constructed}{Total\ Number\ of\ Pixels} * 100 \quad (7)$$

Table.1: BER and PSNR of Decrypted Image

Image	BER	PSNR
Lena	0	Inf
Cameraman	0	Inf
Barbara	0	Inf
Baboon	0	Inf
Pepper	0	Inf

The Table 1 tabulates the BER and PSNR values for various input binary images. The ideal value of BER is 0% and this has been achieved by the proposed algorithm when comparing the original binary image I1 and the decrypted image I2. Since, the ideal value is achieved it need not be

https://dx.doi.org/10.24001/ijaems.3.8.1 *ISSN: 2454-1311*

compared with any algorithm. Similarly, PSNR is infinity for all images which is also the ideal value. Since, the dimensions of the original image is altered the performance measures like Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) may not be used.

VI. CONCLUSION

The security is a major factor in the data transmission. The hacker should not be able to decipher the data even if it is hacked. A novel algorithm is proposed to increase the complexity of the encryption. The complexity of the algorithm has been increased by having 1) Random matrix XORing 2) Number of Keys Used 3) Joining all the Shares and Shares of Various Sizes 4) Wide Range of Mapping Function of the 2 x 2 pixel matrix to a decimal number. The results show that the algorithm is more secure. Also, BER and PSNR value proves that the algorithm decrypts perfectly.

REFERENCES

[1] Xinpeng Zhang, Jing Long, Zichi Wang, Hang Cheng, "Lossless abd Reversible Data Hiing in Encrypted Images with Public-Key Cryptography", IEEE Transactions on Circuits and Systems for Video Technology, Volume 26, Issue 9, Sept 2016

[2] Neha K. Lakde and Dr. P. M. Jawandiya, "A Review of Various Visual Cryptography Schemes", International Journal of Research in Advent Technology, April 2016

[3] AmraneHouas, ZouhirMokhtari, Kamal EddineMelkani, AdelmalikBoussaad, "A Novel Binary Image Encryption Algorithm Based on Diffuse Representation", An International Journal on Engineering Science and Technology, Elsevier, Feb 2016

[4] SudipGhosh, Sayandip De, Santi Prasad Maity, HafizurRahaman, "A Novel Dual Purpose Spatial Domain Algorithm for Digital Image Watermarking and Cryptography using Extended Hamming Code", International Conference on Electrical Information and Communication Technology, IEEE, Jan 2016

[5] Niraj Kumar, Sanjay Agarwal, "An Efficient and Effective Lossless SymmetricKey Cryptography Algorithm for an Image", International Conference on Advances in Engineering and Technology Research, IEEE, Jan 2015

[6] Mona F.M. Mursi, May Salama, Manal Mansour, "Visual Cryptography Schemes: A Comprehensive Survey", International Journal of Emerging Research in Management & Technology, Nov 2014

[7] M. Sukumar Reddy, S. Murali Mohan, "Visual Cryptography Scheme for Secret Image Retrieval", Internation Journal of Computer Science and Network Security", Volume 14, No. 6, June 2014

[8] Chong Fu, Jun-Bin Huang, Ning-Ning Wang, Qi-Bin Hou, Wei-min Lei, "A Symmetric Choas-Based Image Cipher with an Improved Bit-Level Permutation Strategy", Entropy, February 2014

[9] ShekhaChenthara, Deepika M.P., Dr. Varghese Paul, "A Novel Approach on Color Extended VisualCryptography for General Access Structures using Error Diffusion", International Journal of Advanced Research in Computer and Communication Engineering", Volume 3, Issue 2, February 2014

[10] Suhas B. Bhagate, P.J. Kulkarni, "An Overview of Various Visual Cryptogrpahy Schemes", International Journal of Advanced Research in Computer and Communication Engineering", Volume 2, Issue 9, September 2013

[11] Xuehu Yan, Shen Wang, LiLi, Ahmed A. Abd EL-Latif, Zhiqiang Wei, XiamuNiu, "A New Assessment Measure of Shadow Image Quality Based on Error Diffuse Techniques", International Journal of Information Hiding and Multimedia Signal Processing, Volume 4, Number 2, April 2013