Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 01, January-2021

Decision Based Image Encryption Algorithm

Sayyada Fahmeeda Sultana
Department of Computer Science and Engineering
PDA College of Engineering
Kalaburagi, India

Abstract— **In most of the crypto-logical methods, the encrypted data or the cipher texts maintain same statistics of the plain texts, whereas matrix encryption method does not keep the statistics of individual cipher texts. However, it maintains the statistics of block of characters of size m where m is the size of the key matrix. One of the important features of the cipher matrix in Residue Number System (RNS) is that it is highly difficult and time consuming to obtain its inverse by standard inverse algorithms. Matrix in RNS does not have all the eigen values as defined in complex field. The Eigen factors of a matrix are defined as the irreducible factors of the characteristic equation (Eigen function). All the above properties are valid for cipher matrix in Galois Field. The public key is generated by using two types of matrices. One of these matrices is a self-invertible matrix or an orthonormal matrix in Galois field whereas the other matrix is a diagonally dominant matrix. Matrix inversion is very difficult and time consuming when size of matrix and modulo number are large. The computational overhead in generalized Hill cipher can be reduced substantially by using self-invertible matrices. Self-invertible matrices uses less space compared to invertible matrices. In order to overcome this problem, p(modulo) is made very large so that there would be at least p n/2 possible matrices making it extremely difficult for the intruder to find the key matrix. In this paper a Decision Based Image Encryption (DBE) algorithm is proposed that will generate self-invertible matrix for decryption based on DBE algorithm.**

Keywords— Decision Based Image Encryption, Encryption, Binary Coded Decimal (BCD), Encryption, Image, DBE

I. INTRODUCTION

In recent years, the world lives in the age of communications revolution which necessitates multimedia transmission in a secure manner. Encryption is important in transferring images through the communication networks to protect them against reading, alteration of its capacity, adding false information, or concealing part of its contents [1]. Owing to the frequent flow of digital images across the world over the transmission media, it has become essential to secure them from leakages or threatening or brute force attacks. Our proposed encryption scheme is subjected to encrypting on the bases of modified BCD (Binary Coded Decimal) form as BCD representation of number require more than 8 bits to represent all 255 pixel magnitudes. The proposed algorithm uses the following pattern of representing each pixel magnitude, example a=04 is represented as “00000100” in modified BCD form which is same as binary representation. All the pixel magnitude from 0 to 7 follows the same binary representation so example with a=07 follows. Third example is a=72, 72 is represented in modified BCD form as ”0111 0010” and 72 in binary form is written as 1001000. Same pattern follows for all pixel magnitudes between the range 10 to 159. The pixel magnitudes from the range 160 to 255 follows a different pattern as shown in example with value of a as 160, 217, 255. 160 in binary is represented as 10100000, 160 in BCD form is written as 1 00000000 and in modified BCD 160 is represented as 00001000 so as 217 and 255.

II. RELATED WORK

Image encryption algorithms are used to safely store images on cloud and only authorized users can decrypt the image. Chaos-based image encryption has applications in many areas, such as online communications, medical imaging, military communication, etc. Image data contains special properties such as high frequency and high pixel-to-pixel relationships. [23] proposed a new image encryption algorithm, where the gray values of image pixels are mixed and changed to confuse the relationship between the encoded image and the normal image. First Arnold Cat map is used for switching image pixel positions. Authors had explianed with experimental results that the key space is large to resist brute force attack, and that the distribution of gray values for the encoded image has random behavior. [58] proposed an image encryption scheme where the 80-bit secret key and two chaotic logistics maps are used. With the initial conditions of the logistics maps are derived using the key which is external.

Authors have proposed encryption process that includes eight different types of processes to encrypt an image and one of them is used in a given pixel on the logistics map output. [93] introduced image encryption with some propagation effect in the substitution phase by addition and simple serialization. The time taken is longer to process in a single round the encryption. [90]authors proposed cryptographic image-based algorithm with varying control parameters.

The Control parameters included in flipping phase and the key current used in the propagation stage are generated from two chaos maps related to the normal image. Authors showed the result of proposed algorithm can resist all known attacks against diffusion propagation structures effectively. [37] proposed an encryption system that included two parts, mixing chaotic pixels and W7. An anarchic map is used to create a two-way flipping matrix to build a shunt. The flipping matrix has a desirable property and reflects its inverse. Shuffling expands the propagation property and reduces the vertical, horizontal, and diagonal link between adjacent pixels. The number of times each gray level occurs in the image is not changed after the pixel is mixed.

Even the Image Mixing Chart is the same as the Normal Image Chart. [2] The proposed image encryption algorithm, this algorithm is based on the principle of Rubik’s cube to create image pixels. To confuse the relationship between the original images and the encrypted images, the XOR operator

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 01, January-2021

is applied to individual rows and columns of the image using a key. The key itself is turned and applied to rows and columns even from the image. [38] proposed a multipurpose PKI encryption system, the authors provide a solution to meet the increasing requirements for safe image transfer across networks. Supports multilevel encryption based on encryption of various image sizes. [88] worked with an image encryption algorithm based on double helix surveys and chaotic maps. Their main contribution was to perform double helical scan that can effectively mix pixels from the image block. Content-based keys are genes.

III. THE PROPOSED DECISION BASED IMAGE ENCRYPTION (DBIE) ALGORITHM

Algorithm 1 Decision Based Encryption Algorithm

Input: Pixel Magnitude a, Key K
Output: Ciphered Pixel magnitude a_new
Step 1: Count no 10 = 0, temp = 0
Step 2: While a > 9 *do* a = a − 10; *Count no* 10 = *Count no* 10 + 1;
End
Step 3: if Count no 10 == 0 then temp = binary(a, 8); end
Step 4: if Count no 10 < 160 *then*
Temp1 = binary(Count no 10,8);
Temp2 = binary(a, 8); Temp1 = Circular Shift(T emp1, 4);
temp = OR(Temp1, Temp2);
end
Step 5: if Count no 10 ≥ 160 then
Temp1 = binary(count no 10, 8);
Temp2 = binary(a, 8);
Temp1 = Circular Shif t(T emp1, 4);
Temp1 = LeftShift(Temp1, 1);
temp = OR(Temp1, Temp2);
temp = Setbit(temp(4), 1);
end
Step 6: a_new = XOR(temp, K);

Algorithm 2 Decision Based Decryption Algorithm

Input: Ciphered Pixel Magnitude a_new, Key K
Output: Decrypted Pixel Magnitude a
Step 1: temp = XOR(anew, K)
Step 2: D = Getbit(temp(4))
Step 3: C = Getbits(temp(9 ... 5));
a = Getbits(temp(4 ... 1));
Step 4: if D == 0 then
C = binary to decimal(C)
a = binary to decimal(a)
a = (C × 10) + a
end
Step 5: if D! = 0 then a = Setbit(temp(4), 0)
C = binary to decimal(C)
a = binary to decimal(a)
a = ((C + 16) × 10) + a
end
Step 6: return (a)

IV. Results and Analysis

Simulation on the DBE encryption algorithm is done on Akiyo, Big Buck Bunny, Bridge (close), Bridge (Far), Bus, Carphone, Claire, Coastguard, Container, Elephants Dream, Waterfall, Template test video files and around 100 video clips from YouTube. Figure 1 shows the stages of ciphering video frame. The results show that perceptibility of ciphered video is decreased as the object of interest gets encrypted.

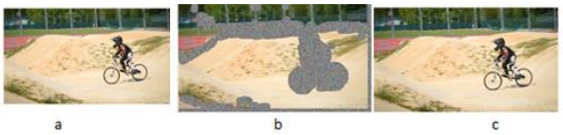

Figure 1: Stages of Video frame encryption (a) Original image (b) Region of Interest Pixels encrypted using DBE algorithm and (c) Decrypted Video frame

Analysis of Results

In this section, the proposed algorithm is subjected to various security analysis and analysis to ensure its accuracy.

TABLE 1: ENCRYPTION AND DECRYPTION TIME FOR SINGLE PIXEL (TIME IN SECONDS)

Stateof Art Algorithms	Encryption Time(s)	Decryption Time (s
Blowfish	0.119	0.119
AES	0.119	0.119
XOR	0.22	0.22
RSA	0.7	2.0
proposed DBE	0.09	0.08

Procession time Table 2 contains the time taken by some of the most commonly used cryptographic algorithms for single pixel, AES, XOR. RSA algorithms are coded in MATLAB16B and Blowfish algorithm in C++. DBE takes less encryption time then other algorithm with less complexity. Table 1 shows the proposed DBE encryption algorithm take least encryption and decryption time as compared to other state of art techniques

Visual Degradation

The maximum signal-to-noise ratio (PSNR) is used to measure the level of optical distortion in the encoded video. With Mean Square Error (MSE), image compression quality can be compared. The MSE describes the separation of the square between the extruded image and the original image, while the PSNR describes a measure of error resolution. A lower MSE value means less error is committed. However, a lower cost of PSNR means higher optical degradation of image encryption. PSNR and MSE were calculated as described in equation1 and equation 2 respectively.

$$P! \qquad (1)$$

Where, M is maximum fluctuation in input image.

$$MSE = \Sigma_{i=1\ to\ m} \Sigma_{j=1\ to\ n} ! \qquad (2)$$

The average PSNR and MSE values for the specific and codec video frame are shown in Table 3. The lower PSNR

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 01, January-2021

values and higher MSE values give a difference between the encoded video and the normal pattern

TABLE 2: COMPARISON OF ORIGINAL FRAME TO CIPHERED FRAME

Comparison of Original frame to Ciphered Frame	**Result**
MSE	2.6488e+03
PSNR	13.9002
Ssimval (Structural similarity index value)	0.3555
VIFP	0.0219

TABLE 3: COMPARISON OF ORIGINAL FRAME TO DECIPHERED FRAME

Comparison of Original frame to decrypted Frame	**Result**
MSE	8.32
PSNR	38.92
Ssimval (Structural similarity index value)	0.9967
VIFP	0.9845

VIFP (Visual Information Fidelity in Pixel)

Domain VIFP relies on two data variables, the statistics between the first and last stage of the detected channel when no separation exists, and the second variable is the data transformed between the input distortion block and the output of the detected system blocks. For the reference image or the left voice, the signal must pass through the visible canal before entering the brain, where the brain data comes from. As is the case with noisy images, the source signal passes through another biased channel before entering a detected channel. Combining the two variables mentioned above, the accuracy is obtained.

Chosen known-plaintext attacks

Figure 2 Histogram analysis shows the effect of selected / known attacks. Normal video frame a) and similar encoding frame b). Because the histogram of part a) and part b) of the objects of interest varies, the proposed technique as opposed to attacks selected / detected by unknown ideas is given limited resources and amount of video over time.

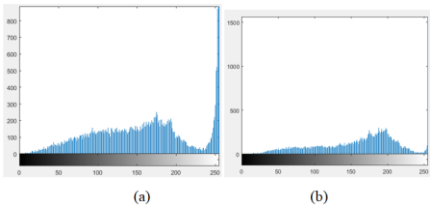

Figure 2: Histogram (a) Original video frame (b) encrypted video frame

Decryption Efficiency

The total difference between the original pixel frames and the recovered frames is approximately 99.8% the same as the original. These results indicate that the decoding process captures normal video with the corresponding 99.8% encryption algorithm generating an error of 0.2%

CONCLUSION

The encrypt ROI through the proposed Decision Based Encryption and Decryption algorithm, the Proposed methodology reduces the encryption and decryption time as only the selected regions need to be encrypted Proposed DBE algorithm is fast robust and secure for any type of data.

REFERENCES

[1] Iskender Agi and Li Gong. An empirical study of secure mpeg video transmissions. In Proceedings of Internet Society Symposium on Network and Distributed Systems Security, pages 137–144. IEEE, 1996.
[2] Zhi-Hong Guan, Fangjun Huang, and Wenjie Guan. Chaos-based image encryption algorithm. Physics Letters A, 346(1-3):153–157, 2005.
[3] Narendra K Pareek, Vinod Patidar, and Krishan K Sud. Image encryption using chaotic logistic map. Image and vision computing, 24(9):926–934, 2006.
[4] Kwok-Wo Wong, Bernie Sin-Hung Kwok, and Wing-Shing Law. A fast image encryption scheme based on chaotic standard map. Physics Letters A, 372(15):2645–2652, 2008.
[5] Yong Wang, Kwok-Wo Wong, Xiaofeng Liao, Tao Xiang, and Guanrong Chen. A chaos-based image encryption algorithm with variable control parameters. Chaos, Solitons & Fractals, 41(4):1773–1783, 2009.
[6] Alireza Jolfaei. Abdolrasoul mirghadri an image encryption approach using chaos and stream cipher. Journal of Theoretical and Applied Information Technology, pp120-122, 2010.
[7] Sufyan T Faraj Al-Janabi. Video encryption based on special huffman coding and rabbit stream cipher. In 2011 Developments in E-systems Engineering, pages 413–418. IEEE, 2011.
[8] PK Kavitha and P Vidhya Saraswathi. Color image encryption: A new public key cryptosystem based on polynomial equation. In International Conference on ISMAC in Computational Vision and Bio-Engineering, pages 69–78. Springer,2018.
[9] Zhenjun Tang, Ye Yang, Shijie Xu, Chunqiang Yu, and Xianquan Zhang. Image encryption with double spiral scans and chaotic maps. Security and Communication Networks, 2019.
[10] Sayyada Fahmeeda, and Dr.Shubhangi D C. ”Privacy Preserved Image Recognition on MSB Encrypted Images.” International Journal of Advanced Research in Computer and Communication Engineering Vol.4, Issue10 (2015), PP. 395-398
[11] Sayyada Fahmeeda and Dr. Shubhangi D C.”Color Image Privacy Preservation using RGB Pixel Numerical Value Shuffling for Cloud Storage”, International Journal Of Research In Electronics and Computer Engineering (IJRECE), Vol. 7, Issue 1 (2019), PP 385-390.
[12] Bruno Whittle. Dialetheism, logical consequence and hierarchy. Analysis, 64(4):318–326, 2004.
[13] Kwok-Wo Wong, Bernie Sin-Hung Kwok, and Wing-Shing Law. A fast image encryption scheme based on chaotic standard map. Physics Letters A, 372(15):2645–2652, 2008.
[14] Chung-Ping Wu and C-C Jay Kuo. Fast encryption methods for audiovisual data confidentiality. In Multimedia Systems and Applications III, volume 4209, pages 284–296. International Society for Optics and Photonics, 2001.
[15] Min Wu and Bede Liu. Watermarking for image authentication. In Proceedings 1998 International Conference on Image Processing. ICIP98 (Cat. No. 98CB36269), volume 2, pages 437–441. IEEE, 1998.
[16] Yue Wu, Sos S Agaian, and Joseph P Noonan. Sudoku associated two dimensional bijections for image scrambling. arXiv preprint arXiv:1207.5856, 2012.
[17] Guodong Ye. Image scrambling encryption algorithm of pixel bit based on chaosmap. Pattern Recognition Letters, 31(5):347–354, 2010.
[18] Siu-Kei Au Yeung, Shuyuan Zhu, and Bing Zeng. Perceptual video encryption using multiple 8× 8 transforms in h. 264 and mpeg-4. In 2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pages 2436–2439. IEEE, 2011.
[19] Lotfi A Zadeh. Fuzzy sets. Information and control, 8(3):338–353, 1965.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 01, January-2021

[20] Wenjun Zeng and Shawmin Lei. Efficient frequency domain selective scrambling of digital video. IEEE Transactions on Multimedia, 5(1):118–129, 2003.

[21] Ming Zhang, Ling Zhang, and Heng-Da Cheng. A neutrosophic approach to image segmentation based on watershed method. Signal Processing, 90(5):1510– 1517, 2010.

[22] Xuyun Zhang, Wanchun Dou, Jian Pei, Surya Nepal, Chi Yang, Chang Liu, and Jinjun Chen. Proximity-aware local-recoding anonymization with mapreduce for scalable big data privacy preservation in cloud. IEEE transactions on computers, 64(8):2293–2307, 2015.

[23] Mazleena Salleh, Subariah Ibrahim, and Ismail Fauzi Isnin. Image encryption algorithm based on chaotic mapping. Jurnal Teknologi, 39(1):1–12, 2012.

[24] Tanvir Habib Sardar and Zahid Ansari. Partition based clustering of large datasets using mapreduce framework: An analysis of recent themes and directions. Future Computing and Informatics Journal, 2018.