An Effective RGB Image Encryption Algorithm Using Chaotic Maps And Memory Cellular Automata

Dr. C. Ramya[1], Rakesh Balaji[2] and S. Karthikeyan[3]
{crm.ece@psgtech.ac.in[1], rakeshbalaji.v@gmail.com[2], karthikeyankumaran1@gmail.com[3]}

Associate Professor, Dept. of ECE PSG College of Technology Coimbatore, India [1], Student, Dept. of ECE PSG College of Technology, Coimbatore, India[2,3]

Abstract. This paper proposes an efficient algorithm for en- ciphering digital RGB images. It makes use of two different dynamical systems. One is chaotic maps and the other is memory cellular automata. The algorithm uses the hash function SHA - 256 on each of the red, green and blue channels of the RGB image for key generation. One notable thing is that the usage of the hash value indicates that the keys generated depend on the plaintext. This key stream created will be used for the generation of the seed values for the chaotic maps we use ie., Logistic-sine and Logistic-tent maps as well as for the generation of the rules for memory cellular automata. The plaintext ie., the input image is first permuted pixel-wise randomly and then undergoes chaotic diffusion. Then the fourth order Memory Cellular Automata (MCA) is applied on it. The algorithm proposed is analyzed with various attacks and their results are discussed..

Keywords: Image Encryption Algorithm, RGB, Memory Cellular Automata.

1 Introduction

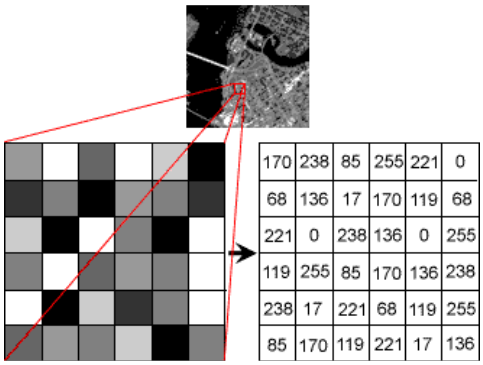

Fig. 1. Gray scale Image and the corresponding intensities in pixels

A. Image Encryption

Image Encryption is simply the encryption process except the fact that the original data here is an image instead of normal text data.

ICCAP 2021, December 07-08, Chennai, India

DOI 10.4108/eai.7-12-2021.2314755

1) What is an image?: An image is a two dimensional matrix of values which range from 0 to 255. Each element in the matrix denotes a pixel and its value indicates the intensity of the pixel that is considered. For example, if an image with dimension 32x32 is considered, then there will be a total of 1024 pixels in the image. Fig. 1 illustrates the intensity values of the pixels in a specific part of the image.

RGB Image – An RGB image is a superposition of three gray scale image matrices namely the red, green and blue channel matrices. Each pixel in an RGB image consists of three different intensity values corresponding to each channel matrix as illustrated in Fig. 2 shows how an RGB image is formed with three channel matrices.

- PRELIMINARIES
- *Hash Function*

Hash function is an algorithm in cryptography which con- verts the variable length data into a cipher text of a fixed size called hash value or message digest.

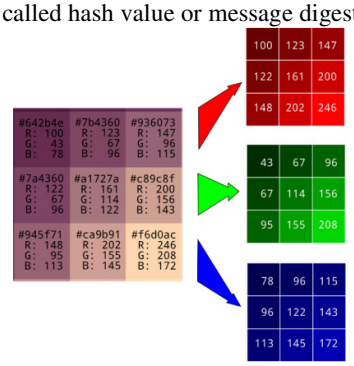

Fig. 2. Various RGB intensity values in an image

SHA-256 (Secure Hash Algorithm, FIPS 182-2) is one of the hash function algorithms which produces the hash value of 256 bits. It doesn't require any key because it is a one way function, meaning the original data cannot be retrieved from the hash value. It is collision resistant and fast to compute. Hash functions are widely used in digital signatures and all the passwords that is entered in the cloud will be hashed and only that message digest will be stored in the server.

- *Chaotic Maps*

Chaotic maps are simple unstable dynamical systems with high sensitivity to initial conditions. These maps show dynam- ical behavior and is a local mechanism for entropy production. This entropy or chaos which is produced can be used to provide the required confusion and diffusion in cryptography. The proposed chaotic system in this paper is the combination of Logistic-Sine map (1) and Logistic-Tent map (2). Its chaotic behaviour has an appropriate usage in image encryption.

$$X_{n+1} = \alpha X_n(1 - X_n) + (4 - \alpha)sin(\pi X_n)/4 \quad (1)$$

- *Memory Cellular Automata*

In Standard Cellular Automata, the state of a cell in the current generation is determined by the neighborhood cells of the generation just before it, whereas, in Memory Cellular Automata, the state of cells in the current generation not only depend on a number of previous generations.

$$C_t = F_1(C_t-1) \oplus F_2(C_t-2) \oplus \quad \oplus F_k-1(C_t-k+1) \oplus (C_t-k)$$

$P_t = F_k{-}1(P_t{-}1) \oplus F_k{-}2(P_t{-}2) \oplus \quad \oplus F_1(P_t{-}k{+}1) \oplus (P_t{-}k)$

the form of a matrix of the same dimension of the original image. It is named as H_1.

$$x'0 = (1/2)(x_0 + h_{1-52}) \quad (5)$$

$$\alpha 0' = (1/2)(\alpha_0 + h_{53-106}) \quad (6)$$

$$x'1 = (1/2)(x_1 + h_{107-158}) \quad (7)$$

$$\alpha 1' = (1/2)(\alpha_1 + h_{159-212}) \quad (8)$$

Step 5–Similarly, the seed values are applied in another chaotic map i.e. Logistic-Tent map and it is recursively iterated for M x N number of times and those values are also reshaped into similar dimension and it is named as H_2.

Step 6–The matrices H_1 and H_2 are bitwise Exored to get the original chaotic matrix for each of the channel matrices. This chaotic matrix will further be used in the Bitwise Exor Chaotic Diffusion process.

Proposed Methodology

- *Encryption Process*
- *Seed Generation:* Step 1–Initially, the original image of dimension M x N is separated into corresponding three channel matrices ie., red, green and blue channels. The obtained channel matrices are then fed to the hash function. The hash function used for key generation is SHA – 256 hash function which gives the hash value or the message digest that consists of 256 bits. For each of the channels Step 2 to Step 13 is carried out.

Step 2–The first 212 bits of the hashes is split into 4 different parts as $h_{1\text{-}52}$, $h_{53\text{-}106}$, $h_{107\text{-}158}$, $h_{159\text{-}212}$. These parts of hash values are used for the calculation of seed values that is to be used in the chaotic map for the generation of the chaotic matrix and the keys for memory cellular automata.

Step 3–x0, 0, x1, and 1 are the initial secret keys that is used to find the seeds of the LS map, LT map as well as for the rules for MCA. h_{ij} in the seed calculation equations denote the decimal conversion of the substring taking from the i^{th} bit to j^{th} bit of the hash value.

Step 4–The seed values are thus obtained from the equations (5)-(9). Once the seed values are obtained, firstly, they are substituted in the logical-sine map and iterated for M x N number of times. The values thus obtained are reshaped in

- *Bit-Wise EXOR Chaotic Diffusion :* The original image of dimension M x N has to be bitwise XORed with the chaotic matrix.

Step 7–Firstly, the LS map (1) is iterated recursively for (M*N + 500) times with the control parameter ’1 and the seed x’1. Ignore the first 500 values and then take the next M x N

values that is obtained. The reason that the first 500 values are ignored is that those values will not exhibit the desired chaos that is needed for encryption

Step 8–Now, reshape those M x N values into a 2-D matrix which is in the same dimension as that of the image matrix. Thus the chaotic matrix is obtained. Though the reshaped matrix is obtained the issue here is that all of those values in the chaotic matrix will range within [0, 1].

Step 9–To map the values in the chaotic matrix to the domain [0, 255], the Equation (5) is used. Thus, the required chaotic matrix H is obtained.

$$H = (Sx1015) mod 256 \quad (9)$$

$$P1 = H \oplus P \quad (10)$$

$$P2 = G_s d(P1) \quad (11)$$

- *Transition Rules of MCA:* Step 10–A k^{th} order reversible MCA needs k-1 number of transition rules and k previous configuration to obtain the new configuration. These transition rules are generated as follows,

Step 11–Firstly, the control parameter ’0 and the seed x’0 calculated are fed to the LS map (1) and recursively iterated for a number of times (more than 500) to avoid the transient effect. It is continuously iterated and the next 4x3 values that are obtained are used for the sequence E.

Step 12–The values in sequence E is mapped from the domain [0, 1] to the domain [0, 255] to get the sequence Q.

$$Q = (Ex1015) mod 256 \quad (12)$$

Step 13–Then Q is converted into binary sequence K which will contain 4 x 3 x 8 = 384 bits. This sequence K is split into k1, k2, k3 (128 bits each) which are the three transition rules for the 4th order MCA. Note that a 32 bit rule is used because r = 2 i.e. a 5-bit neighborhood is considered and hence $(2^7)^7$ rule sets are possible.

- *Fourth Order MCA:* Step 14–The permuted image P2 is divided into 4 equal 2-D matrices of dimension M/2 x N/2. Those blocks are named as p1, p2, p3, p4 respectively. These blocks are then converted into a binary sequence of length M/2 x N/2 x 8 = 2MN. Now the MCA generation mechanism is applied using the transition rules. These configurations are converted into their decimal for and reshaped to their original dimension to get the encrypted image.

The steps 2 to 14 are done for each of the channel matrices. And finally those 3 channel matrices are combined to get the RGB encrypted image.

$$C = Ht, xt(P2) \quad (13)$$

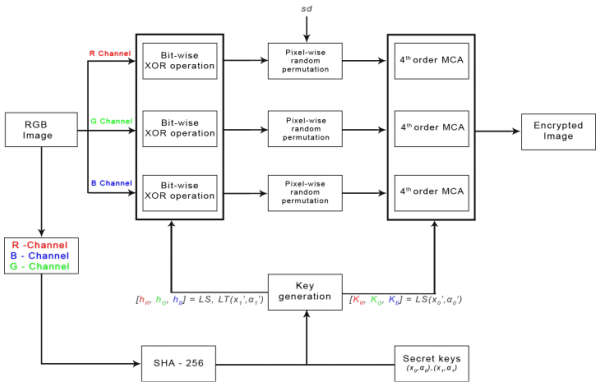

Fig. 3. Encryption Process

- *Decryption Process*

To properly recover the original image, a total of six parameters must be transmitted to the decryption side. These parameters include the seeds and system parameters of the LS map (x0; 0; x1, and 1), the seed of the scramble order (sd), and the 256-bit hash value of the original image.

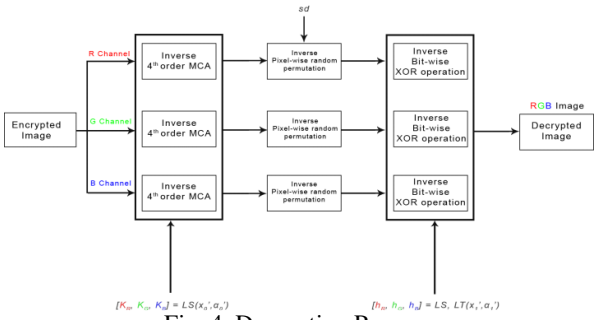

Fig. 4. Decryption Process

Results And Discussion

The proposed algorithm is tested with various RGB images and some of them are shown in Fig. 5.

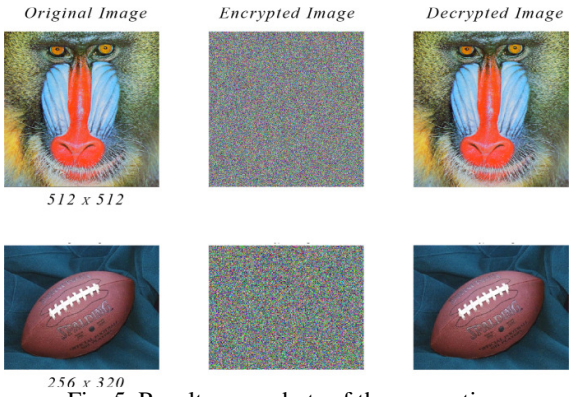

Fig. 5. Result screenshots of the encryption

A. Robustness Analysis

- *Occlusion Attack:* Ciphered images are inevitably af- fected by occlusions during transmission. Quality of the decrypted image reduces as the occlusion size increases. Therefore an encryption scheme should be robust enough to resist such occlusion attacks. The results are shown in Table II.

TABLE I ROBUSTNESS AND QUALITY MEASUREMENTS FOR PROPOSED ALGORITHM AGAINST THE ADDITION OF NOISES AND ENHANCEMENT ATTACKS

Attacks	PSNR	NCC	SSIM
Salt and Pepper Noise(var=0.05)	21.2452	0.92288	0.71316
Salt and Pepper Noise(var=0.1)	18.1113	0.84883	0.54747
Salt and Pepper Noise(var=0.2)	15.1409	0.72351	0.37013
Salt and Pepper Noise(var=0.3)	13.3912	0.60932	0.26316
Gaussian Noise(var=0.01)	14.2601	0.655	0.28621
Gaussian Noise(var=0.05)	11.5497	0.42257	0.14018
Gaussian Noise(var=0.1)	10.6399	0.33047	0.1057
Gaussian Blur(var=0.3)	28.1858	0.98452	0.91285
Gaussian Blur(var=0.4)	17.7876	0.84115	0.49867
Gaussian Blur(var=0.5)	13.638	0.60362	0.21343
Brightness attack(increased by 1%)	25.7499	0.96956	0.86264
Brightness attack(increased by 5%)	19.1025	0.85594	0.59983
Brightness attack(increased by 10%)	16.4569	0.74801	0.43993
Brightness attack(increased by 20%)	14.3571	0.60806	0.30345
Brightness attack(decreased by 1%)	25.1572	0.97144	0.84601
Brightness attack(decreased by 5%)	18.1082	0.85322	0.53018
Brightness attack(decreased by 10%)	15.3587	0.7324	0.3568
Brightness attack(decreased by 20%)	12.3692	0.49269	0.17625

of digital images. SSIM is used to measure the similarity between two images. The SSIM values for the proposed algorithm with attacks are shown in Table I.

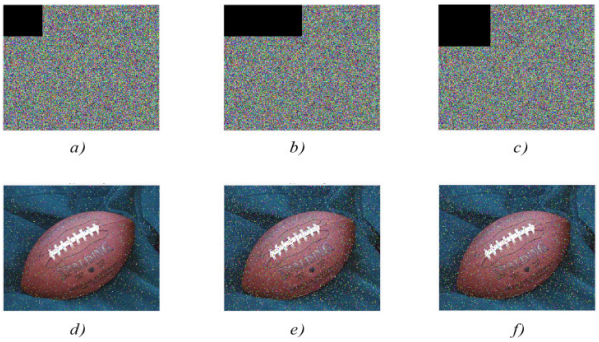

Fig. 6. Test of Occlusion Attacks: Encrypted image with a)1/16 b)1/8 c)1/9 data loss and their corresponding decrypted images

TABLE II
ROBUSTNESS ANALYSIS - OCCLUSION ATTACKS

Fraction of Data loss	PSNR	NCC	SSIM
1/16	20.3652		0.68
	0.87098	968	
1/8	17.3659		0.51
	0.76884	941	
1/9	17.8887		0.55
	0.78972	301	

- *NCC Analysis:* The Normalized Cross Correla- tion(NCC) values for the decrypted image with the non- geometric attacks are taken to anlayse the robustness of the proposed algorithm. Robustness and quality measurements of the proposed algorithm with non-geometric attacks are listed in Table I.

- *PSNR Analysis:* The Peak Signal-to-Noise Ratio (PSNR) is employed to measure the quality of the proposed method. The PSNR values for the proposed algorithm with attacks are shown in Table I.

- *SSIM Analysis:* The Structural Similarity Index Measure (SSIM) is a method used to predict the perceived quality

Conclusion

This paper exhibits a robust RGB image encryption algo- rithm. It makes use of two familiar dynamic systems: chaotic maps and memory cellular automata. This algorithm comprises of three major steps which are key generation, diffusion- confusion and fourth order memory cellular automata. For the key generation part, the hash function SHA-256 is used for the channel matrices. The advantage is that it has a large keyspace that prevents it from brute-force attacks. In the diffusion-confusion stage, Bit-wise EXOR and pixel-wise random permutation takes place. This is followed by 1-D fourth order memory cellular automata. Key space analysis and robustness analysis is done to evaluate the performance of the proposed algorithm and found encouraging results.

References

[1] Seyed Alireza Hosseini and Seyed Reza Kamel, ”Fast Encryption of RGB Color Digital Images Based On Elementary Cellular Automata Using three Processors”, Second International Congress on Technology, Communication and Knowledge (ICTCK2015),2015.

[2] Yicong Zhou, Long Bao, C.L. Philip Chen , ”A new 1D chaotic system for image encryption”, Signal Processing, vol. 97, pp. 172–182, Apr. 2014.

[3] A. Souyah and K. M. Faraoun , ”Fast and efficient randomized encryption scheme for digital images based on quadtree decomposition and reversible memory cellular automata”, Nonlinear Dynamics, vol. 84, no. 2, pp. 715–732, Apr. 2016.

[4] Md Nazish Aslam, Akram Belazi, Sofiane Kharbech,Muhammad Talha,Wei Xiang, ”Fourth Order MCA and Chaos-based Image Encryption Scheme”, IEEE Access, Vol. 7, pp. 66395 – 66409, April 2019.

[5] C. Priya, C. Ramya ”Robust and Secure Video Watermarking Based on Cellular Automata and Singular Value Decomposition for Copyright Protection”, IEEE Access, Vol. 7, pp. 66395 – 66409, April 2020.

[6] Kiruthika, C., S. Lavanya Prabha, and M. Neelamegam. "Different aspects of polyester polymer concrete for sustainable construction." Materials Today: Proceedings 43 (2021): 1622-1625.

[7] D. S. Vijayan, A. Leema Rose, S. Arvindan, J. Revathy, C. Amuthadevi, “Automation systems in smart buildings: a review”, Journal of Ambient Intelligence and Humanized Computing https://doi.org/10.1007/s12652-HYPERLINK "https://doi.org/10.1007/s12652-020-02666-9"020-02666-9

[8] M. Tholkapiyan, A.Mohan, Vijayan.D.S , “A survey of recent studieson chlorophyll variation in Indian coastal waters”, IOP Conf. Series: Materials Science and Engineering 993 (2020) 012041, doi:10.1088/1757-899X/993/1/012041.