Color Image Privacy Preservation using RGB Pixel Numerical Value Shuffling for Cloud Storage

Sayyada Fahmeeda Sultana[1], Shubhangi DC[2]
[1] PDA College of Engineering
[2] VTU PG Center, Kalaburagi
(E-mail: sayyadafahmeeda@gmail.com)

***Abstract*—**Image privacy preservation is one of the key issues to be considered before storing on cloud or uploading on Online Social Media (OSNs) as images are the most reveling data. Encryption is a technique by which unauthorized users are prevented from understanding Original image contents. Encryption methods for enhancing security for Image contents have gained huge importance resent era to breach from misuse and security concerns of confidential and personal images which may be misused by the unauthorized users. In this paper, the properties of RGB Image are used to construct special encrypted Image and further reverse procedure is used to decrypt image varying perceptibility. RGB plains of images are scattered to perform encryption. The proposed color image encryption algorithm using Shuffling of Red Green and Blue plain's (RGB) pixel numerical values for images of varying sizes. The proposed Image encryption algorithm IES (Image Encryption using RGB Shuffling) works by dividing the image into three horizontal splits the first split becomes the R plain, second split as G plain and the third split as B plain of Ciphered image, further each split performs the shuffle of numerical pixel values from RGB plain. Proposed encryption algorithm is the faster then the other state of art encryption algorithms. Algorithm provide the number of pixel change rate (NPCR) as 99.64 with the speed of encryption as $1.94749*10^3$ KB/sec.

Keywords— *Image Encryption; Image Encryption Using RGB Shuffling (IES) algorithm; RGB plain Shuffling; Cloud; Online Social Media*

INTRODUCTION

Cloud Storage and Sharing of images through Online Social Media is accresent broad application broad applications becoming an vital part of today's life due to the requirement of huge storage, timely access to the Images are rising in recent decade. It also delay less message communications and offline message sharing such as private information on social media (YouTube), blogging (Twitter), between user's regardless of their geographical location. There are numerous OSNs with specially for photo sharing (like, Flickr), college, travel, business etc. OSNs helps families and friends to stay connected, maintain their social relations in a more convenient way than traditional conversations like phone, mails and emails, and hence have gained wide popularity among social groups. Images are the most revealing data that need to be protected such that unauthorized users are not allowed to view or download images. User's Image privacy is at risk when exploited for adversarial exposure, e.g., accessing private images without permissions, illegally selling, profiling the image owner, etc. The risks are spectacularly increasing especially when users are needed to include their real names and profiles in the OSN applications; leading users vulnerable to image privacy breach. A secure and efficient privacy preservation scheme suitable for sharing images on OSNs are highly needed.

Image Privacy can be better achieved using Cryptography, which today needs to use advanced mathematical procedures during encryption and decryption process. Encryption algorithms are becoming time consuming and more complex. The two main broad approaches to encryption, are symmetric key and asymmetric key algorithms. Symmetric-key algorithm [18] is a class of algorithm for encryption that uses the same cipher keys for both encryption of plain data and decryption of cipher data. Another, approach pixel diffusion and chaotic confusion [19] that performs repetitive steps of permutations and changes are used to achieve security.

This paper proposes a Color Image encryption technique through an encryption algorithm for images of varying sizes through shuffling of RGB plain numerical values. The algorithm encrypts and decrypts the images based on the RGB plain numerical values without complex calculation and key management. The organization of paper: related work discussed in section II, Methodology for encryption and decryption explain in section III, Simulation result and discussion is performed in section IV. Paper is concluded with future work in section V.

RELATED WORK

Inconsistencies that appear in distributed social network when treating images and access policies separately proposed solution to solve. Showed an access police, each time a photo is re-shared, the access policy will travel together with the image [1]. Social network operators are increasingly publishing and sharing social network data with third party consumers. The published social network data contain potentially sensitive information about users and their relationships. Authors have presented a high level framework for social network publishing threat analysis, threat model and quantified and classified the background knowledge that is potentially used by adversaries to breach privacy of the published social network data. Also proposed number of methods, approaches, strategies and techniques in privacy-preserving social network data publishing. [7,8,9,14].The transposition and reshuffling of the Red Green Blue plain values of the image in steps have been used by authors to perform ciphering and deciphering of image[3].

Image scrambler using knight's moving rules (from the game of chess), along with a chaos-based permutation, in order to transpose original image's pixels between RGB channel is proposed in [4]. Chaos-based image encryption algorithm for generating random permutations as a part of the elements from the beginning of the permutation will have large values and a part of the elements from the end of the permutation will have small ones, so the shift factor of the permutation will be large [10].

Double Scrambling of image is performed first horizontally and the result of horizontal scrambling as input to vertical scrambling [15]. Sudoku Associated Image Scrambler using these Sudoku associated two dimensional bijections, by using a scrambling key to control these bijections in a parametric way [16].

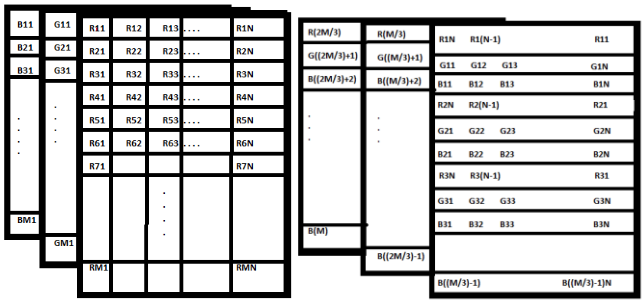
Single chaos map used to implement gray scrambling encryption of an image, in which the pixel values(0-255) tha tare distributed evenly, the positions of pixels are permutated. Authors transform statistical characteristic of original image information, to increase the difficulties of an unauthorized users to break the encryption [17].

PROPOSED METHODOLOGY

The image under encryption under have its RGB plain, the completed image RGB plains, for every pixel the G and B plain numerical value extracted and assigned R plain from G plain to the first neighbour pixel and plain B numerical value to the second neighbour pixel once all the assignments have reached image boundaries the same process is repeated for Green and Blue plains to obtain cipher Image. The ciphering of images for this research will be done by using the RBG pixel values shuffling only. In the proposed method there are no changes for pixel bit values of images used neither, pixel expansion at the end of the encryption and the decryption. Numerical values of the pixels are misplaced from their original positions and the RGB values are shuffled to obtain the ciphered images, the total change in the image and image size (dimensions) is zero.

The R-G-B components are considered the characteristics of a pixel, With the proposed method in this paper, the encryption of a image was ultimately done shuffling the RGB pixels numerical values.

The process of encryption is shown pictorially in figure(1), pixel representation of original image figure (1a), encrypted image figure(1b). Algorithm 1 Image Encryption Using RGB Shuffling (IES) is used for image encryption process and Algorithm 2 is used for decryption process.



(a) (b)

Figure(1) Pictorial representation RGB plain of (a) Original Image (b) Encryption Algorithm

A. Mathematical Representation of Proposed Algorithm

Original Image $\boldsymbol{A}(\boldsymbol{nXmX3})$ equ(1) n,m are the dimensions of image its RGB plains of image are shown by $\boldsymbol{A_r}$, $\boldsymbol{A_g}$, $\boldsymbol{A_b}$, matrices by equ(2,3,4) respectively. r,g,b represents the three plain of image

$$\boldsymbol{A} = \begin{bmatrix} \boldsymbol{A1,1\ B1,1\ C1,1\ \ldots\ldots\ M1,m} \\ \boldsymbol{A2,1\ B2,2\ C2,3\ \ldots\ldots\ M2,m} \\ . \\ . \\ . \\ \boldsymbol{An,1\ Bn,2\ Cn,3\ \ldots\ldots\ M,n,m} \end{bmatrix} \quad \ldots \quad (\mathbf{1})$$

$$\boldsymbol{A_r} = \begin{bmatrix} \boldsymbol{A1,1,r\ B1,1,r\ C1,1,r\ \ldots\ldots\ M1,m,r} \\ \boldsymbol{A2,1,r\ B2,2,r\ C2,3,r\ \ldots\ldots\ M2,m,r} \\ . \\ . \\ . \\ \boldsymbol{An,1,r\ Bn,2,r\ Cn,3,r\ \ldots\ldots\ M,n,m,r} \end{bmatrix} \quad \ldots \quad (\mathbf{2})$$

$$\boldsymbol{A_g} = \begin{bmatrix} \boldsymbol{A1,1,g\ B1,1,g\ C1,1,g\ \ldots\ldots\ M1,m,g} \\ \boldsymbol{A2,1,g\ B2,2,g\ C2,3,g\ \ldots\ldots\ M2,m,g} \\ . \\ . \\ . \\ \boldsymbol{An,1,g\ Bn,2,g\ Cn,3,g\ \ldots\ldots\ M,n,m,g} \end{bmatrix} \quad \ldots \quad (\mathbf{3})$$

$$\boldsymbol{A_b} = \begin{bmatrix} \boldsymbol{A1,1,b\ B1,1,b\ C1,1,b\ \ldots\ldots\ M1,m,b} \\ \boldsymbol{A2,1,b\ B2,2,b\ C2,3,b\ \ldots\ldots\ M2,m,b} \\ . \\ . \\ . \\ \boldsymbol{An,1,b\ Bn,2,b\ Cn,3,b\ \ldots\ldots\ M,n,m,b} \end{bmatrix} \quad \ldots \quad (\mathbf{4})$$

Ciphered images $\boldsymbol{A'}$ equ(5) its RGB plains are shown by matrices $\boldsymbol{A'_r}, \boldsymbol{A'_g}, \boldsymbol{A'_b}$with equ(6,7,8) respectively.

$$\boldsymbol{A'} = \begin{bmatrix} \boldsymbol{A1,1\ B1,1\ C1,1\ \ldots\ldots\ M1,m} \\ \boldsymbol{A2,1\ B2,2\ C2,3\ \ldots\ldots\ M2,m} \\ . \\ . \\ . \\ \boldsymbol{An,1\ Bn,2\ Cn,3\ \ldots\ldots\ M,n,m} \end{bmatrix} \quad \ldots \quad (\mathbf{5})$$

$$A'_r = \begin{bmatrix} A1,1,r\ B1,1,r\ C1,1,r & \ldots.. & M1,m,r \\ A1,1,g\ B1,2,g\ C1,3,g & \ldots.. & M1,m,g \\ A1,1,b\ B1,2,b\ C1,3,b & \ldots.. & M1,m,b \\ A2,1,r\ B2,2,r\ C2,3,r & \ldots.. & M2,m,r \\ A2,1,g\ B2,2,g\ C2,3,g & \ldots.. & M2,m,g \\ A2,1,b\ B2,2,b\ C2,3,b & \ldots.. & M2,m,b \\ & . & \\ & . & \\ & . & \\ Ay,1,z\ By,2,z\ Cy,3,z & \ldots.. & My,m,z \end{bmatrix} \quad \ldots \quad (6)$$

$z = (r,g,b)$ can be any value between r or g or b, $y = \frac{n}{3}$, y represents $\frac{1}{3}$ of original image's rows

$$A'_g = \begin{bmatrix} Ay+1,1,r\ By+1,1,r\ Cy+1,1,r & \ldots & My+1,m,r \\ Ay+1,1,g\ By+1,2,g\ Cy+1,3,g & \ldots & My+1,m,g \\ Ay+1,1,b\ By+1,2,b\ Cy+1,3,b & \ldots & My+1,m,b \\ Ay+2,1,r\ By+2,2,r\ Cy+2,3,r & \ldots & My+2,m,r \\ Ay+2,1,g\ By+2,2,g\ Cy+2,3,g & \ldots & My+2,m,g \\ Ay+2,1,b\ By+2,2,b\ Cy+2,3,b & \ldots & My+2,m,b \\ & . & \\ & . & \\ & . & \\ Ax,1,z\ Bx,2,z\ Cx,3,z & \ldots & Mx,m,z \end{bmatrix} \quad \ldots \quad (7)$$

$x = \frac{2n}{3}$, x represents $\frac{1}{3}$ of original image's rows

$$A'_b = \begin{bmatrix} Ax+1,1,r\ Bx+1,1,r\ Cx+1,1,r & \ldots & Mx+1,m,r \\ Ax+1,1,g\ Bx+1,2,g\ Cx+1,3,g & \ldots & Mx+1,m,g \\ Ax+1,1,b\ Bx+1,2,b\ Cx+1,3,b & \ldots & Mx+1,m,b \\ Ax+2,1,r\ Bx+2,2,r\ Cx+2,3,r & \ldots & Mx+2,m,r \\ Ax+2,1,g\ Bx+2,2,g\ Cx+2,3,g & \ldots & Mx+2,m,g \\ Ax+2,1,b\ Bx+2,2,b\ Cx+2,3,b & \ldots & Mx+2,m,b \\ & . & \\ & . & \\ & . & \\ An,1,z\ Bn,2,z\ Cn,3,z & \ldots.. & Mn,m,z \end{bmatrix}$$

Image Encryption Using RGB Shuffling (IES) Algorithm for Encryption and Decryption

---

Algorithm 1: Image Encryption Using RGB Shuffling (IES)

Input: I (Orignial image), Image Size $(M\ X\ N)$
Output: CI (Ciphered Image)
Step 1: Read I, M, N
Step 2: $CI = I$
Step3: for $i = 1:(M/3)$
  for $j = 1:N$
  $CI(b1,j,R) = I(i,j,R)$;
  $CI(b2,j,R) = I(i,j,G)$;
  $CI(b3,j,R) = I(i,j,B)$;
 end
  end
[where $b1$ is the current pixel, $b2, b3$ represents 1st and 2nd neighbour pixels of $b1$ pixel, R, G, B (are Red, Green, Blue plains of a image)]
Step 4: for $i = (round((M)/3)):(round((2*M)/3))$
  for $j = 1:N$
  $CI(b1,j,G) = I(i,j,R)$;
  $CI(b2,j,G) = I(i,j,G)$;
  $CI(b3,j,G) = I(i,j,B)$;
 end
  end
Step 5: for $i = (round((2*M)/3)):M$
  for $j = 1:N$
  $CI(b1,j,B) = I(i,j,R)$;
  $CI(b2,j,B) = I(i,j,G)$;
  $CI(b3,j,B) = I(i,j,B)$;
 end
  end
Step 6: Convert CI into image format
Step 7: CI
Step 8: Stop

Algorithm 2: Image Decryption

Input: CI (Ciphered Image), Image Size $(M\ X\ N)$
Output: DI (Decrypted Image)
Step 1: Read CI, M, N
Step 2: $I = CI$
Step3: for $i = 1:m$
count $= 0$;
for $j = 1:n$
count $=$ count $+ 1$;
$r(i, count) = CI(i,j,R)$;
$g(i, count) = CI(i,j,G)$;
$b(i, count) = CI(i,j,B)$;
end
end
[where : [Count keep track of number columes]
Step 6: $DI(:,:,R) = r, DI(:,:,G) = g, DI(:,:,B) = b$ (: − for all pixels $(M\ X\ N)$)
Step 7: DI (with RGB plain)
Step 8: Stop

RESULTS AND DISCUSSION

The proposed video Encryption algorithm is tested on more than 100 short video clips of varying Image sizes, and also on DAVIS color image data set containing 50 categories images each category contain 50 images. The code for this algorithm was implemented on MATLAB 2016. The result of after applying algorithm1 encryption algorithm and their corresponding histograms are shown in figure (2). Figure (2a) shows the color image of size 1280 X 760 pixels. Figure (2b) shows the ciphered image. figure (2c) indicate the decrypted image generated using Algorithm (2). Histogram of original and ciphered images shown in figure (2d and 2e) are totally different figure(2f) shows the Histogram decrypted image.

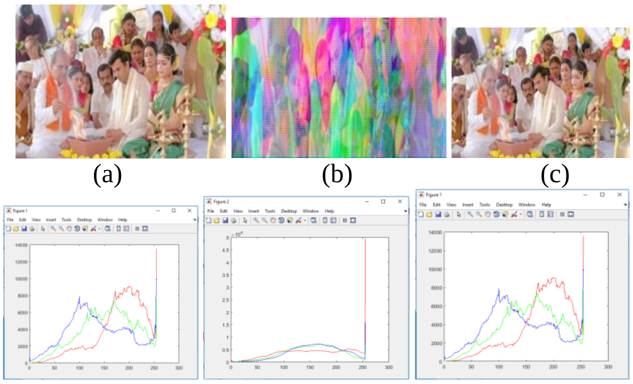


Figure 2. (a) Plain Image (b) Ciphered Image (c) Decrypted Image (d) Histogram of plain Image with different color channel (e) Histogram of ciphered image (f) Histogram of decrypted Image

B. *Comparison and Analysis of Results*

As requirement to validate image encryption the output encrypted image must be different from plain image and also should provide ability to perform feature extraction so that content based retrieved on encrypted images can be performed Cloud Storage. Result Comparisons can be performed from statistical point, Histogram analysis. To quantify the result, in addition to visual assessment, statistical estimators are used, most commonly.

Adjacent Pixels Correlation Coefficients (APCC) Analysis : From plain image, any randomly chosen pixels are strongly correlated with their adjacent ones (diagonally, vertically, or horizontally). An efficient image encryption algorithm must minimize this correlation. Figure 2 show the distributions of correlation horizontally (a), vertically (b), and diagonally (c) with corresponding adjacent pixels for the Vegetable image, for same vegetable image when encrypted using the proposed method horizontal(d), vertical (e), diagonal (f).

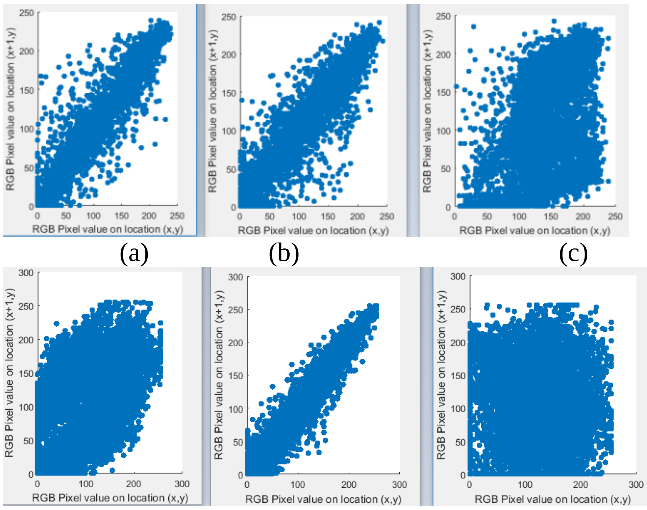


Figure (3) Plot of distribution Correlation of adjacent pixels of Vegetables Original and Ciphered image (a) Adjacent pixels Horizontally, (b) Adjacent pixels vertically, and(c) Adjacent pixels diagonally and (d),(e) and (f) shows Horizontal, vertical and diagonal adjacent pixels of ciphered image

As shown in figure(3) shows the Analysis of correlation distribution of adjacent pixels of original and ciphered image. Analyses of correlation disribution of adjacent pixels of original and ciphered image are different.

The Table 1 below shows the APCCs for Benchmark images at different plains (RGB) for both original and encrypted Images

Table 1. Adjacent Pixel Correlation Coefficient Analysis

Pixel Adjacency	Image	Color Channel	Vegetable Image	Lenna Image	Baboon Image	Difference[(Original)-Random Permutation and RGB Shuffling(RPS)] images
Vertical	Original	Red	0.9652	0.9790	0.9239	18.4%
		Green	0.9688	0.9686	0.8823	
		Blue	0.9508	0.9302	0.928	
	Random Permutation and RGB Shuffling(RPS)	**Red**	**0.7671**	**0.7837**	**0.7357**	
		Green	**0.7507**	**0.7781**	**0.7557**	
		Blue	**0.7551**	**0.7808**	**0.7337**	
Horizontal	Original	Red	0.9610	0.9881	0.9129	43.8%
		Green	0.9685	0.9821	0.8655	
		Blue	0.9396	0.9544	0.9226	
	Random Permutation and RGB Shuffling(RPS)	**Red**	**0.2473**	**0.6080**	**0.4793**	
		Green	**0.3919**	**0.6838**	**0.6319**	
		Blue	**0.4205**	**0.7168**	**0.3697**	
Diagonal	Original	Red	0.9325	0.9689	0.8718	43.37%
		Green	0.9430	0.9552	0.7997	
		Blue	0.9047	0.9155	0.8805	
	Random Permutation and RGB Shuffling(RPS)	**Red**	**0.2235**	**0.5944**	**0.4167**	
		Green	**0.3695**	**0.6624**	**0.5909**	
		Blue	**0.4086**	**0.7004**	**0.3020**	

Unified Average Changing Intensity (UACI) and Number Of Pixel Change Rate (NPCR) measures: Calculation of UACI evaluated using equ(1), if two totally different images are considered for UACI comparison maximum approximately estimated as UACIC = 33.4635%.

$$UACI(IM_P, IM_S, c) = \left(\frac{1}{WXH} \sum_{I=1}^{W} \sum_{J=1}^{H} \frac{IM_P(I,J,C) - IM_S(I,J,C)}{255} \right) x100 \qquad (9)$$

Table (2) summarizes the result of NPCR and UACI for test

Authors	NPCR	UACI	Speed(KB/s)
Dascalescu and Boriga[10]	99.431	25.032	$12.5*10^3$
Dalhoum et al.[15]	90.126	NaN	NaN
Wu et al.[16]	94.163	NaN	NaN
Ye[17]	93.676	NaN	NaN
AdrianViorel Diaconu et. al.[4]	99.489	29.006	117.028
Quist-Aphetsi Kester[3]	98.95	17.98	170.03
Proposed Algorithm: Random Permutation and RGB Shuffling(RPS)	99.64	27.86	$1.94749*10^3$

The Table(2) above shows the results of different Image encryption algorithms with their statistical calculation the proposed video encryption algorithm gives high NPCR and Speed which is very efficient for video encryption. Further, the proposed algorithm can be used for content based feature extraction.

CONCLUSION

Image Encryption performed by Displacement of pixel RGB numerical values to their adjacent pixels and dividing the image into three split horizontal each split becomes the R or G or B plain of the ciphered image. The proposed algorithm encrypts the image without any key management, with no extra mathematical calculations. As image after encryption retain its original data content based retrieval on encrypted data can be quickly performed. The proposed IES algorithm is fast in computation, it can also be used to encrypt video frames. The proposed IES image encryption algorithm can be further extended using machine learning algorithms.

REFERENCES

[1]. Pablo Picazo-Sanchez, Raúl Pardo, Gerardo Schneider, "Secure Photo Sharing in Social Networks", IFIP International Conference on ICT Systems Security and Privacy Protection, ICT Systems Security and Privacy Protection, May 2017, Pages 79-92, https://doi.org/10.1007/978-3-319-58469-0_6

[2]. Ziad E.Dawahdeh, Shahrul N.Yaakob, RozmieRazif bin Othman, "A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher", Journal of King Saud University - Computer and Information Sciences,Volume 30, Issue 3, July 2018, Pages 349-355, https://doi.org/10.1016/j.jksuci.2017.06.004

[3]. Quist-Aphetsi Kester, "Image Encryption based on the RGB PIXEL Transposition and Shuffling", I. J. Computer Network and Information Security, July, 2013, Pages 43-50, https://doi.org/10.5815/ijcnis.2013.07.05

[4]. Adrian-Viorel Diaconu, Alexandru Costea, Marius-Aurel Costea, "Color Image Scrambling Technique Based on Transposition of Pixels between RGB Channels Using Knight's Moving Rules and Digital Chaotic Map", Hindawi Publishing Corporation Mathematical Problems in Engineering Volume 2014, Pages 1-15, http://dx.doi.org/10.1155/2014/932875

[5]. Amnesh Goel, Nidhi Chandra, "A Technique for Image Encryption with Combination of Pixel Rearrangement Scheme Based On Sorting Group-Wise Of RGB Values and Explosive Inter-Pixel Displacement", I.J. Image, Graphics and Signal Processing, Feb. 2012, Pages 16-22, https://doi.org/10.5815/ijigsp.2012.02.03

[6]. Xingyuan Wang, Xiaoqiang Zhu, Yingqian Zhang, "An Image Encryption Algorithm Based on Josephus Traversing and Mixed Chaotic Map", IEEE Access, Volume 6, May 2018, Pages 23733-23746, https://doi.org/10.1109/ACCESS.2018.2805847

[7]. Jyothi Vadisala, Valli Kumari Vatsavayi, "Challenges in Social Network Data Privacy", International Journal of Computational Intelligence Research,Volume 13, Number 2017, Pages. 965-979.

[8]. Warit Sirichotedumrong, Tatsuya Chuman, Shoko Imaizumi, Hitoshi Kiya, "Grayscale-based Block Scrambling Image Encryption for Social Networking Services", arxiv:1806.03787v1, june 2018, Pages 1-6, https://doi.org/978-1-5386-1737-3/18

[9]. Ahmet Emir Dirik, Nasir Memon, "Selective Robust Image Encryption for Social Networks", International Conference on Multimedia Communications, Services and Security MCSS 2013: Multimedia Communications, Services and Security, 2013, Pages 71-8, DOI: https://doi.org/10.1007/978-3-642-38559-9_7

[10]. Ana Cristina Dascalescu , Radu Eugen Boriga, "A novel fast chaos-based algorithm for generating random permutations with high shift factor suitable for image scrambling", Nonlinear Dynamics, Volume 74, Issue 1-2, 2013 ,Pages 307–318, https://doi.org/10.1007/s11071-013-0969-6

[11]. Boddu Ramya Sri, Shrija Madhu, "A Novel Method for Encryption of Images based on Displacement of RGB Pixels", National Conference on Emerging Trends in Computing (NCETC-2K17), Godavari Institute of Engineering and Technology, Rajahmundry, April 2017, Pages 4-7.

[12]. Dong Wang, Chin-Chen Chang, Yining Liu, Guoxiang Song, Yunbo Liu, "Digital Image Scrambling Algorithm Based on Chaotic Sequence and Decomposition and Recombination of Pixel Values", International Journal of Network Security, Volume 17, Issue 3, May 2015, Pages 322-327.

[13]. Dharna Singhai, Chetan Gupta, "A Review on Various Image Encryption Technique using AES and Random RGB Substitution", International Journal of Advanced Research in Computer and Communication Engineering, Volume 7, Issue 1, January 2018, Pages 210-215, https://doi.org/10.17148/IJARCCE.2018.7135

[14]. Tatsuya Chuman, Kenta Iida, Hitoshi Kiya, "Image Manipulation on Social Media for Encryption-then-Compression Systems", Proceedings of APSIPA Annual Summit and Conference, Malaysia, December 2017, Pages 1-6.

[15]. A.L.A.Dalhoum, B.A.Mahafzah, A.A.Awwad, I.Aldamari, A. Ortega, and M. Alfonseca, "Digital image scrambling using 2D cellular automata", IEEE Transactionson Multimedia,vol.19, no.4, 2012, Pages 28–36, https://doi.org/10.1109/MMUL.2011.54

[16]. Y. Wu, S. S. Agaian, and J. P. Noonan, "Sudoku associated two dimensional bijections for image scrambling", http://arxiv .org/abs/1207.5856, source: arXiv.

[17]. G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map", Pattern Recognition Letters, volume.31, no.5, 2010, Pages 347–354, https://doi.org/10.1016/j.patrec.2009.11.008

[18]. Nicolas Courtois, Josef Pieprzyk, "Cryptanalysis of Block Ciphers with Over defined Systems of Equations", ASIACRYPT 2002, Pages 267–287.

[19]. M. Salleh, S Ibrahim and I.F. Isnin, "Image encryption algorithm based on chaotic mapping", JurnalTeknologi, Universiti Teknologi Malaysia, 2003, Pages 1-12

[20]. Sayyada Fahmeeda Sultana, Shubhangi D C, "Video Encryption Algorithm and Key Management using Perfect Shuffle", Int. Journal of Engineering Research and Application , Volume 7, Issue 7, July 2017, Pages 01-05, https://doi.org/10.9790/9622-0707030105

[21]. Sayyada Fahmeeda Sultana, Shubhangi D C, "Authentication, Tamper Localization And Rectification Algorithm With Privacy Preservation Of Image For The Cloud Using HMAC", Ictact Journal On Image And Video Processing, Volume: 08, Issue 02, November 2017, Pages 1660-1664, https://doi.org/10.21917/ijivp.2017.0233