



A NOVEL IMAGE CRYPTOGRAPHY USING UES

Dr. Sri Ram Chandra Polisetty^{1*}, Dr. S.V.R.K.Rao²

Dr. G. Venkateswara Rao³

^{1,2} Faculty of Engineering, Godavari Institute of Engineering and Technology
(A), Rajahmundry, A.P. India.

³ Faculty of Engineering, GITAM-Deemed to be University, Visakhapatnam,
A.P., India

Corresponding Author: Dr. Sri Ram Chandra Polisetty (dr.psr@yahoo.com)

Abstract

In this paper, an image encryption method using Ultramodern Encryption Standard (UES) is envisioned. In this method, the encryption key is spawned by prolic series and then the original image is encrypted using the UES cryptosystem. This approach not just decreases the time complexity of the algorithm yet additionally adds the confusion and diffusion capacities, which makes the encrypted pictures developed by the UES approach resistant to the differential assaults. The key space of UES cryptosystem is large enough to fight the brute-force attacks. This approach is so subtle to the initial values and input picture so the little changes in these values can prompt critical changes in the encrypted picture. The model results depicted in the further sections ensures that slight changes in original image and key could result significant changes in the encrypted image and finally the original image cannot be accessed.

Keywords: UES, Cryptosystem, Encryption, Decryption, Image Encryption, Prolic Series

1. Introduction

The outright developed digitalization in recent days is playing a fundamental role in digital image transmission viz., legislature, medical, military, banking, finance sectors. In transferring such critical pictures across the digital transmission medium may sometimes get under the control of the intruder who can tamper its contents and may lead to declination of war, wrong treatment etc... in military and medical sectors respectively. Securing such significant images is possible through image encryption. Hence a high end image encryption technique with low time complexity is to be applied. In preference transmission of images between sender and receiver has to be done in short span of time, because irreparable damages may be happened, if the delay is more than the threshold.

A few assessment standards are to be considered in image encryption viz., "Histogram Analysis", "Adjacent Pixels Correlation Coefficient (APCC)", "Number of Pixels Change Rate (NPCR)" and "Unified Average Changing Intensity (UACI)". On the off chance that the upsides of these standards meet the ideal hope, this implies that the algorithm can resist the statistical and differential attacks [1]. Furthermore, an image encryption technique should have a major key space and high affectability to the underlying conditions to oppose the brute-force attacks [1].

Earlier authors [5] enrich the properties of confusion and diffusion making use of discrete exponential chaotic maps, which in turn will be useful for design a scheme for the resistance to static, differential and grey code attacks. Some authors [6] employed Arnold cat mapping is used to identify the location of the image pixels in the spatial domain, from there the output signal is preprocessed. This mapping technique is encrypted the signal in a pixel to pixel manner. This resultant algorithm has three fold advantages like using large space which avoids resistant attacks, has an appropriate statistical feature and also very sensitive to the various keys.

This paper proposes to use Ultramodern Encryption Standard (UES) cryptosystem for image encryption and decryption. UES is a new symmetric stream cipher that uses prolic series number for generating set of keys, binary and gray code operations for encryption and decryption processes. If an intruder captures contents of the message, it is a challenging one to decipher the contents for the reason that multilevel cipher rounds are used in this cryptosystem [2].

The content of this research article is organized as in following three sections; Section 2 describes the methodology of Image Cryptography using UES, Results and Discussion are incorporated in Section 3, Finally Section 4 provides the conclusions and future scope.

2. Architecture Of Image Cryptography Using Ues

UES is an Ultramodern Encryption Standard cryptosystem that uses prolic series number for generating set of keys, corresponding image gets encrypted and decrypted using binary and gray code operations. The number that satisfies the relation $T_n = n \times (n + 1) \ n \geq 0$ said as Prolic Series, where T_n is n^{th} term of the prolic series [2]. Encryption process starts by considering an image file as an input, the corresponding HEX file of this image is extracted. Now the entire HEX file is divided into block of two hexadecimal digits each i.e., a block of 8 binary digits and given as an input to UES encryption process.

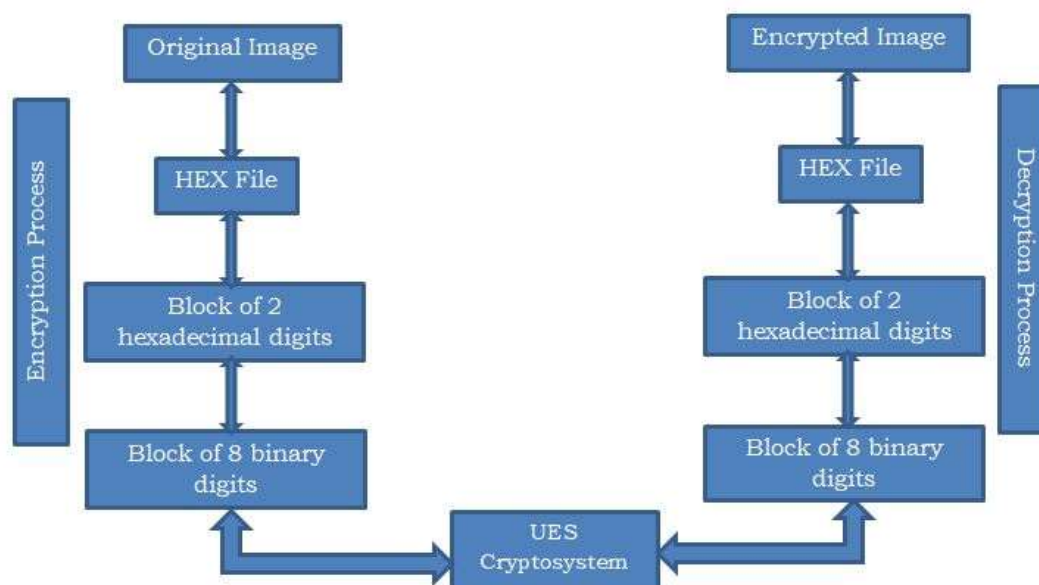


Figure 1: Architecture of Image Cryptography using UES Cryptosystem

2.1 Generation of essential keys in UES using Prolic Series

In the context of cryptography, a key is essentially a very big number preferably in terms of binary. Keys are a fundamental component of cryptography that can be used in encryption, decryption, hashing etc. The detailed flowchart for generation of keys in UES is described as follows [2].

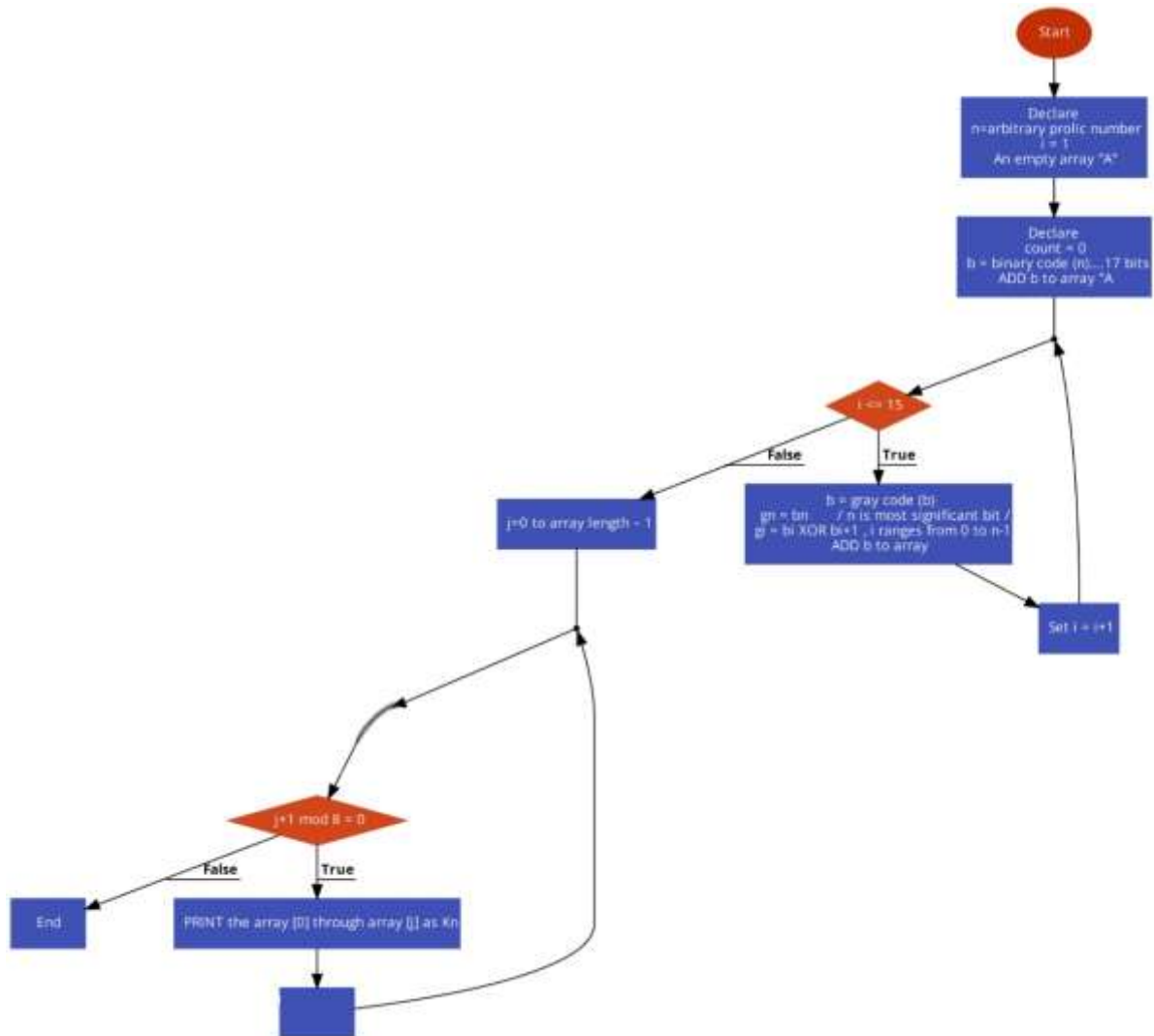


Figure 2: Flowchart showing Key Generation Process in UES

2.2 Image Encryption by means of UES

The image encryption method of UES ignites by considering the 256×256 image as an input. Now the corresponding HEX file of the image is determined and whole HEX file is divided as a block of 2 hexadecimal digits each. 8 bit binary digits of 2 hexadecimal values are computed and there after it goes through 16 rounds of encryption where 32 squares of key 8 bits each are being utilized. At last the cycle would end by working two output transformations utilizing 2 squares of key 8 bits each. Abstract model of encryption and one round of encryption are exemplified in the Fig2 and Fig3 correspondingly.

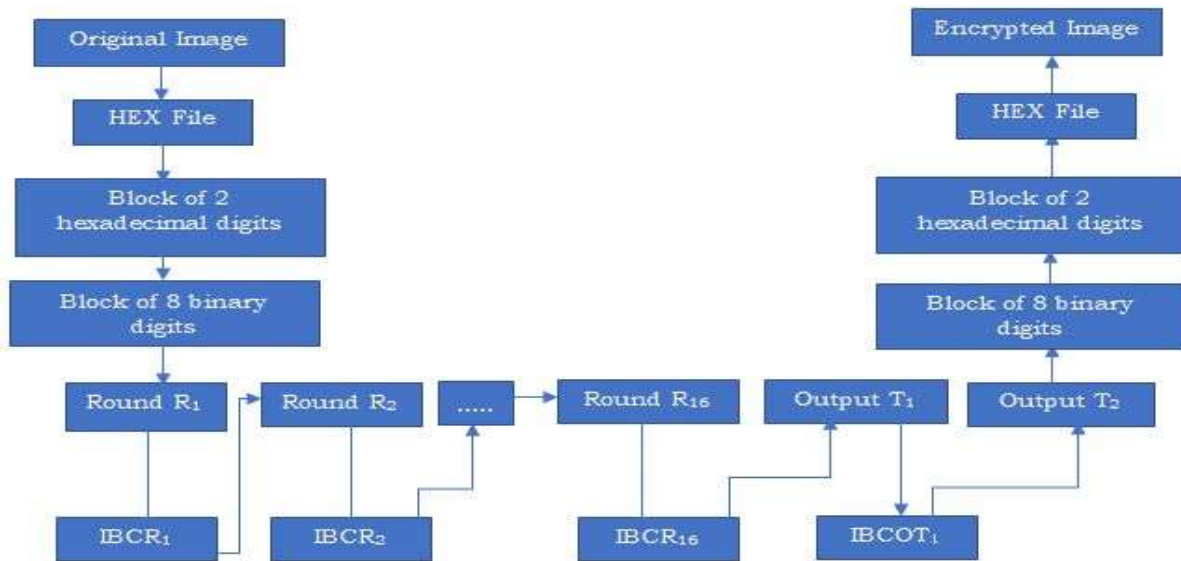


Figure 3: Block Diagram of Image Encryption using UES

Where, $IBCR_{\#}$ specifies Intermediate Binary Cipher of the equivalent round, Output $T_{\#}$ specifies Output Transformation and $IBCOT_{\#}$ specifies Intermediate Binary Cipher of the Output Transformation.

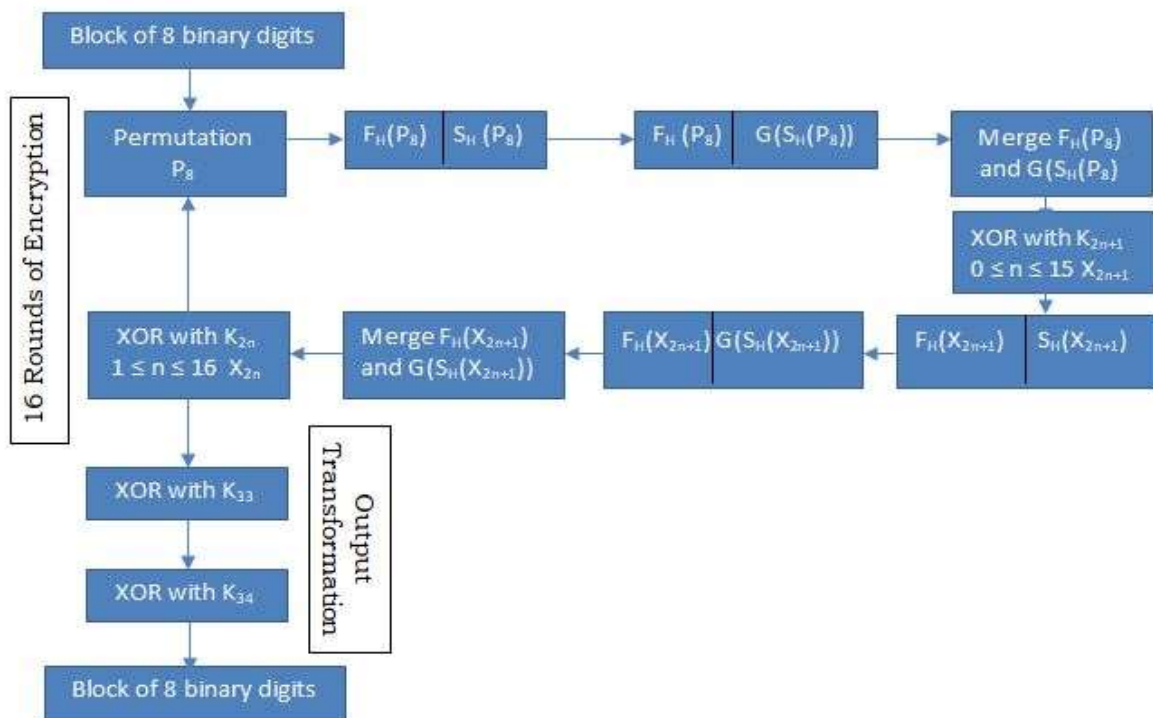


Figure 4: Detailed execution of one round of Image Encryption

Where, F_H : First Half; S_H : Second Half; G : Gray code

2.3 Image Decryption by means of UES

The image decryption method of UES ignites by considering the 256×256 encrypted image as an input. Now the corresponding HEX file of the image is determined and whole HEX file is divided as a block of 2 hexadecimal digits each. 8 bit binary digits of 2 hexadecimal values

are computed and there after it goes through 16 rounds of decryption where 32 squares of key 8 bits each are being utilized. Abstract model of decryption and one round of decryption are exemplified in the Fig4 and Fig5 correspondingly.

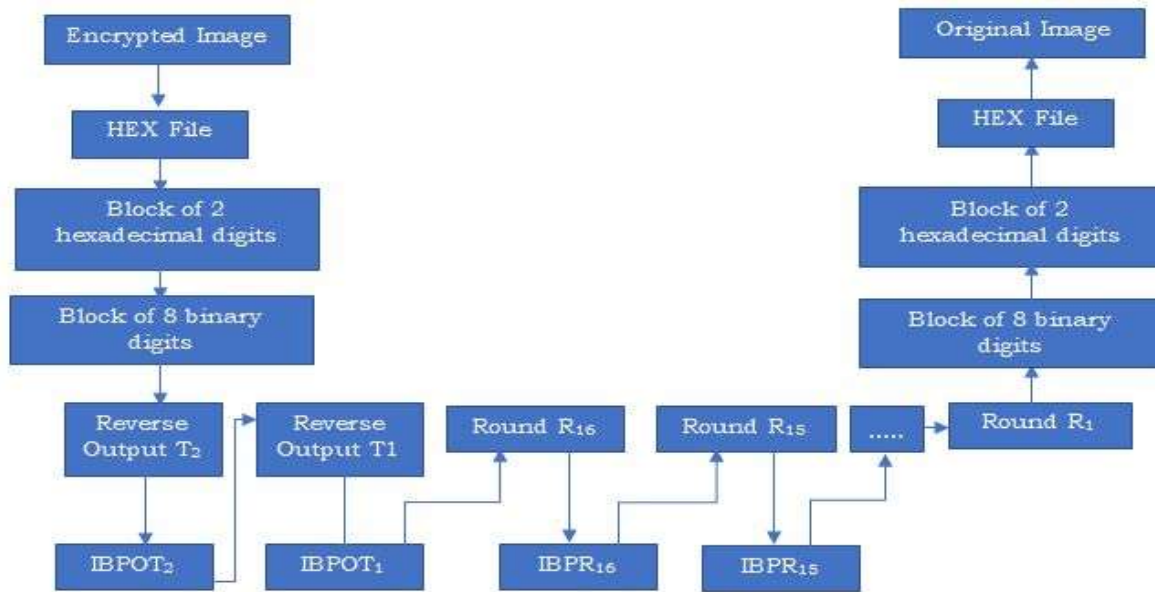


Figure 5: Block Diagram of Image Decryption using UES

Where Reverse Output T#: Reverse Output Transformation, IBPOT#: Intermediate Binary Plaintext corresponding to Output Transformation and IBPR#: Intermediate Binary Plaintext corresponding to Round number.

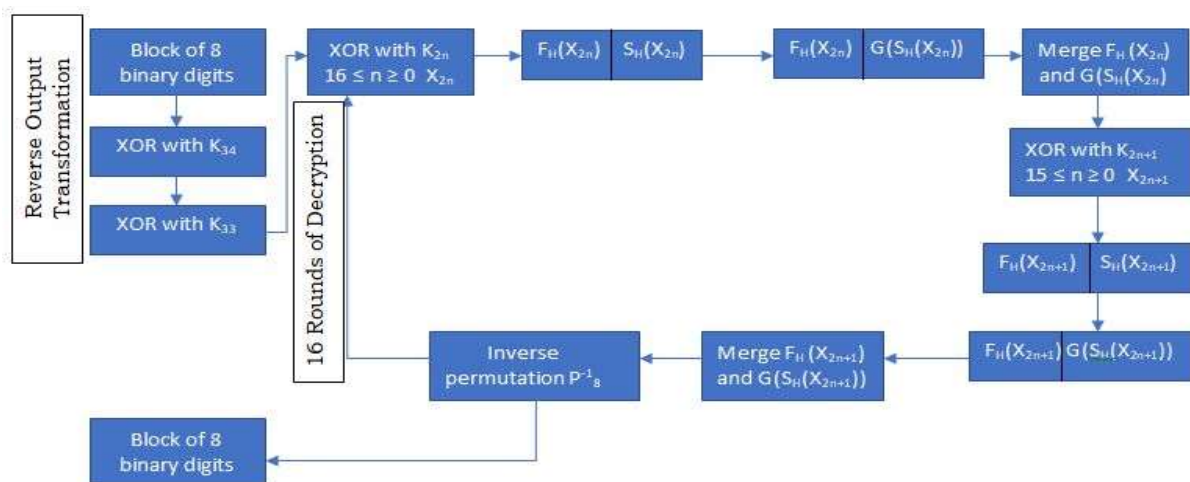


Figure 6: Detailed execution of one round of Image Decryption

Where F_H : First Half S_H : Second Half G : Gray code


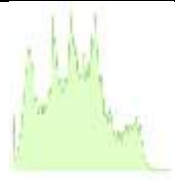


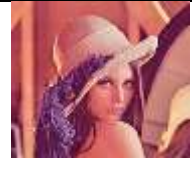











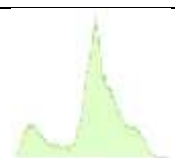



3. Results And Analysis

The histogram investigation is one of the most straight-forward strategies for showing the image encryption efficiency. Since a decent picture encryption technique will in general scramble an original image to irregular like, it is wanted to see a consistently dispersed

histogram for an encrypted image. Section 3.1 shows a few histograms from the original and encrypted images respectively.

3.1 Histogram analysis of the original and encrypted images

Table 1 Histogram Analysis of Original and Encrypted Images

Image No.	A Original Image	B Histogram of A	C Encrypted Image of A	D Histogram of C	E Decrypted Image of C
1					
2					
3					
4					

Observing the images 1 through 4, histograms of the images encrypted is consistent and significantly differs from the original image. Column A and E of table1 clearly depicts that image encryption and decryption is functioning properly. Hence, it is evident that the original image is resistant to certain intruder’s attacks by using UES Cryptosystem.

Chi-Square test is one of the assessment methods used to measure the histogram’s uniformity and is defined as follows:

$$X^2 = \sum_{k=1}^{256} \frac{(V_k - 256)^2}{256} \dots\dots\dots 1$$

Where count of gray scale areas is denoted by *k* and each area’s repetition by *V_k*.

Table 2 Chi-square test values of Images before and after Encryption

Chi-square/ Image Number	1	2	3	4
Image before encryption	29,384	213843	145214	54125
Image encrypted using UES Cryptosystem	245.1245	251.3256	235.8469	269.3256

Thus the histogram analysis of the images before and after encryption depicted in Table 1 is consistent. The Chi-Square test values in table 2 holds good for justification of histogram’s consistency.

3.2 Adjacent Pixels Correlation Coefficient (APCC)

In image encryption algorithm we generally adopt adjacent pixels correlation coefficient technique to find out the correlation between the pixels. In plane images be closer pixel is correlated with that doesn't pixel in vertical horizontal and diagonal orientation for assessment of correlation parameter. As expected, pixels in high performance image encryption algorithm are very poorly correlated and the correlation score is very close to null value. For the correlation calculation $r(x, y)$ where x and y denotes values of the grey scale images corresponds to the two adjacent pixels for N number of chosen adjacent pixels were considered. In brevity, for a well encrypted image the correlation coefficient of adjacent pixel is very low and close to zero, in this case the intruder cannot get access to the information [13]. Section 3.2 briefly describes about the equations used to evaluate the correlation between the two adjacent pixels and their tabulated results.

$$E(X) = \frac{1}{N} \sum_{i=1}^N X_i \dots\dots\dots 2$$

$$cov(x, y) = \frac{1}{N} \sum_{i=1}^N (X_i - E(X))(Y_i - E(Y)) \dots\dots\dots 3$$

$$D(X) = \frac{1}{N} \sum_{i=1}^N (X_i - E(X))^2 \dots\dots\dots 4$$

$$r(x, y) = \frac{cov(x, y)}{\sqrt{D(X)}\sqrt{D(Y)}} \dots\dots\dots 5$$

Table 3: Comparison results of APCC: UES and other methods

Image Number	APCC	Ref. [5]	Ref. [8]	Ref. [9]	Ref. [10]	Ref. [11]	Ref. [12]	Ref. [13]	UES Cryptosystem
1	H	0.02086	0.082	0.012	0.01183	0.0014	0.000707	0.005	0.0026999
	V	0.02458	0.040	0.027	0.00016	0.0055	0.00216	0.011	0.00199
	D	0.009666	0.005	0.007	0.01480	0.000146	0.014886	0.023	0.0002896
2	H	0.02115	0.0941	0.0123	0.01251	0.009841	0.009955	0.00412	0.001584
	V	0.02451	0.0257	0.0324	0.00658	0.00564	0.004915	0.00556	0.0045213
	D	0.00851	0.00215	0.0045	0.0214	0.00159	0.05541	0.0365	0.001547
3	H	0.00658	0.00625	0.01480	0.00851	0.014886	0.01183	0.0257	0.005123
	V	0.01183	0.01480	0.02458	0.05541	0.02958	0.0214	0.0214	0.003564
	D	0.01251	0.0257	0.00551	0.014886	0.00625	0.01251	0.05541	0.001874
4	H	0.014886	0.00851	0.01251	0.00321	0.02210	0.00851	0.02458	0.00214
	V	0.05541	0.00625	0.00851	0.0257	0.00658	0.01480	0.00625	0.001699
	D	0.02458	0.00658	0.01183	0.01480	0.014886	0.02458	0.01183	0.0008398

H: Horizontal V: Vertical D: Diagonal

Observing APCC of the images 1 through 4 in table3, it goes closer to zero in UES i.e., all bordering pixels studied in the test are weakly correlated than the other methods reported. Hence, it is evident that the UES cryptosystem is a good one and resistant to certain intruder’s attacks.

3.3 NPCR and UACI

The rate of change of number of pixels in the encrypted image as soon as single pixel in the original image is altered: said as NPCR and it can be worked out via the following equation:

$$NPCR = \frac{\sum_{(i,j)} D(i,j)}{W \times H} \times 100 \% \dots\dots\dots 6$$

The average intensity of disparities between the original image and encrypted image is usually computed by Unified Average Changing Intensity (UACI).

$$UACI = \frac{1}{W \times H} \left[\sum_{(i,j)} \frac{C_1(i,j) - C_2(i,j)}{255} \right] \times 100 \dots\dots\dots 7$$

Where D (i, j) is defined as

$$D(i,j) = \begin{cases} 0, & \text{if } C_1(i,j) = C_2(i,j) \\ 1, & \text{if } C_1(i,j) \neq C_2(i,j) \end{cases} \dots\dots\dots 8$$

W and H are the width and height of encrypted image.

A plain picture is first encoded and afterward, a pixel in that picture is arbitrarily chosen and flipped. The altered image is encoded again utilizing the equivalent keys in order to create another encrypted image. At last, the NPCR and UACI values are determined. An experimental simulation was done on a computer and it was revealed that NPCR and UCAI of the UES are 99.75% and 33.56 correspondingly, where their ideal values are 99.61% and 33.46% correspondingly.

Table 4: Comparison results of NPCR and UCAI: UES and other methods

Cryptosystem	NPCR %	UCAI %
Zhang et al. 2nd round [8]	21.50	2.50
Zhou et al. 2nd round [9]	25.00	8.50
Guanrong Chen 5th round [10]	50.20	25.20
Khanzadi et al. [11]	99.52	33.14
Wang [12]	97.62	32.90
Etemadi et al. [13]	99.70	29.30
UES	99.75	33.56

3.4 Key Space

The total number of possibilities of keys used in the encryption process is defined as key space. Literature in [7, 13] says that, a key space of 2¹⁰⁰ is sufficient to call a cryptosystem as

a good one. UES key space can be given 2^{272} , which makes the system impractical to the brute-force attack and no other attack can pushover it.

4. Conclusions and Future Scope

Protecting images in today's digital world has become paramount because of rapid increase in the digital communication. In order to protect the images an image encryption method using Ultramodern Encryption Standard (UES) is anticipated in this paper. The series of operations embodied in UES for image encryption not only reduce the time complexity of the cryptosystem but also adds diffusion and confusion ability to UES and is resistant to certain intruder's attacks. The key space of UES is

The histogram of original and encrypted images were tabulated in table 1 and justified by chi-square test. The APCC results of encrypted images depicted in table 3 is evident that the pixels of images encrypted by UES are weakly correlated than the other methods reported in literature. The comparative results depicted in table 4 regarding NPCR and UACI values shows that substantial variations are noticed in the encrypted image by a swift change in original image. Hence, it is evident that the UES cryptosystem is better one than the other methods reported in literature as well it is resistant to certain intruder's attacks.

References

- [1] Kumari M, Gupta S, Sardana P (2017) A survey of image encryption algorithms. 3D Res 8(4):37
- [2] P.Sri Ram Chandra, G.Venkateswara, G.V.Swamy, „Ultramodern Encryption Standard Cryptosystem Using Prolic Series for secure data transmission“““ „International Journal of Latest Engineering Research and Applications(IJLERA)ISSN 2455-7137 Volume_02,Issue 11,November-2017,pp-29-35.
- [3] A. DONNER, B. ROSNER, On inferences concerning a common correlation coefficient, J. R. Stat. Soc. C-Appl. Stat., 29, 1, pp. 69-76, 1980. doi: 10.2307/2346412
- [4] Y. WU, Y. ZHOU, S. AGAIAN, J.P. NOONAN, 2D Sudoku associated bijection for image scrambling, Inf. Sci., 327, pp. 91-109, 2016. doi: 10.1016/j.ins.2015.08.013.
- [5] Zhang, L.; Liao, X.; Wang, X.: An image encryption approach based on chaotic maps. Chaos Solitons Fractals 24(3), 759–765 (2005)
- [6] Guan Zhi-Hong, Huang Fangjun, Guan Wenjie (2005) Chaos-based image encryption algorithm. Phys Lett A 346(1-3):153–157
- [7] Alvarez, G.; Li, S.: Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurcation Chaos 16(8), 2129– 2151 (2006)
- [8] Linhua, Z; Liao, X.; Wang, X.: An image encryption approach based on chaotic maps. Chaos Solitons Fractals 24(3), 759–765 (2005)
- [9] Zhou, Q.;WoWong, K.; Liao, X.; Xiang, T.; Hu, Y.: Parallel image encryption algorithm based on discretized chaoticmap. Chaos Solitons Fractals 38(4), 1081–1092 (2008)
- [10] Guarnong, C; Mao, Y.; Chui, C.K.: A symmetric image encryption scheme based on 3D chaotic Cat maps. Chaos Solitons Fractals 21(3), 749–761 (2004)
- [11] Khanzadi, H.;Omam, M.A.;Lotfifar, F.; Eshghi,M.: Image encryption based on gyration transforms using chaotic maps. In: Signal Processing (ICSP), 2010 IEEE 10th International Conference on 2608–2612 (2010)

- [12] Wang, Y.; Wong, K.W.; Liao, X.; Chen, G.: A new chaos-based fast image encryption algorithm. *Appl. Soft Comput.* 11, 514–522 (2009)
- [13] Borujeni, S.E.; Eshghi, M.: Chaotic image encryption design using tompkins-paige algorithm. *Hindawi Publishing Corporation Mathematical Problem in Engineering* vol. 200, p. 22 (2009)
- [14] Alireza Arab, Mohammad Javad Rostami, Behnam Ghavami: An image encryption method based on chaos system and AES algorithm *The Journal of Supercomputing* (2019) 75:6663–6682
- [15] Himan Khanzadi Mohammad Eshghi Shahram Etemadi Borujeni :Image Encryption Using Random Bit Sequence Based on Chaotic Maps. *Arab J Sci Eng* (2014) 39:1039–1047