# Image encryption scheme in public key cryptography based on cubic pells quadratic case

**Raghunandan K R[1], Ganesh Aithal[2], Surendra Shetty[3], Bhavya K[4]**
[1,3,4]NMAM Institute of Technology, Nitte, Affiliated to Visvesaraya Technological University, India
[2]Shri Madhwa Vadiraja Institute of Technology & Management Bantakal, Visvesaraya Technological University, India

**Article Info**

***Article history:***

Received Jan 20, 2020
Revised Mar 25, 2020
Accepted Apr 10, 2020

***Keywords:***

Avalanche effect
Correlation analysis
Differerential analysis
Entropy
Image encryption
Pell's equation
Quadratic equation

## ABSTRACT

Cryptography systems face new threats with the transformation of time and technology. Each innovation tries to contest challenges posed by the previous system by analyzing approaches that are able to provide impressive outcomes. The prime aim of this work is to urge ways in which the concept of Pell's equation can be used in Public key Cryptography techniques. The main aim of this approach is secure and can be computed very fast. Using Cubic Pell's equation defined in Quadratic Case, a secure public key technique for Key generation process is showcased. The paper highlights that a key generation time of proposed scheme using Pell's Quadratic case equation is fast compared to existing methods.The strength and quality of the proposed method is proved and analyzed by obtaining the results of entropy, differential analysis, correlation analysis and avalanche effect. The superiority of the proposed method over the conventional AES and DES is confirmed by a 50% increase in the execution speed and shows that Standard diviation and Entropy analysis of proposed scheme gives immunity to guess the encryption key and also it is hard to deduce the private key from public key using diffrential analysis.

***Corresponding Author:***

Raghunandan K R,
Department of Computer Science and Engineering,
NMAM Institute of Technology, Nitte,
Visvesaraya Technological University, India.
Email: raghunandan@nitte.edu.in

## 1. INTRODUCTION

At present, with the quick progress of new innovation and the exchange of advanced information, sensitive data should be able to confront criminal ambushes. With this point of view, numerous alternative ways to deal with exchange of information have been proposed in the area of cryptography. Many of which use mathematics and number theory in the first place [1].

Conventionally, there are two kinds of systems in Cryptography. System that use one key for both encipher and decipher are referred as “Symmetric Cryptosystems”. The distinguishing factor in these systems is the usage of a single key shared at the sender's end for encryption and at the receiver's end for decryption. However, the evolution of communication technologies shown disadvantages of such an arrangement. Since a single key is involved in encryption, decryption and key management is problematic. “Public Key Cryptosystems” (PKC) were introduced to address the weaknesses of the existing system. This arrangement is based on the usage of two different keys, one for enciphering and another for deciphering at the receiver's siide [2, 3]. Research carried out in the field of Private key cryptography and in the field of image encryption is summarized in the following paragraph.

Alvarez et al. at paper [4] explored the effectiveness of medical image encryption and found that the algorithm can be breakable using proposed attack procedure. In [5] Muhaya cryptanalyzed the encryption scheme and found that image encryption is suffering from password guessing attack.

Paper [6] suggested permutation key can be recovered using differential cryptanalysis which indicating the insecurity nature of enciphering scheme. In view of the above said shortcomings highlighted in [4-6] can be resolved using the proposed methodology, since it make use of public key infrastructure. This paper concentrates on public key, especially using cubic Pell's eaquation and quadratic equation which is explained briefly in next section.

## 2. BASIC CONCEPTS TO PRELIMINARY

### 2.1. Pell's equation

Pell's equation was invented by John Pell. Euler [7], who titled the equation as "Pell's equation" was oblivious to the way that this equation had been analyzed by an Indian mathematician named Brahmagupta. In fact, several other mathematicians like Bhaskara II produced solutions to the equation [8]. Pell's equation is a significant topic of algebraic number theory that includes quadratic structures [9]. This equation has a prolonged historical backdrop, and included numerous methodologies before a conclusive theory was developed [10, 11]. In this paper the polynomial arrangements of the Pell's equation is defined as

$$x^2 - dy^2 = 1 \tag{1}$$

where $d$ is a non-negative, non-square integer and $x$ and $y$ can have infinite positive integral solutions. We refer to this as the polynomial Pell equation. Cubic-degree version of the same can be written as,

$$x^3 - dy^3 = k \tag{2}$$

where $d$ is a non-cubic number. Notably, the arrangements of such equations are not abundant, nor do they display the pleasant structure witnessed in the quadratic case.This paper introduces a novel methodology which concedes a hypothesis practically identical to the quadratic case adaptation which is discussed in next section.

### 2.2. Quadratic equations

A 2nd order polynomial equation used in a single variable $x$ is typically termed as a "Quadratic" equation. The 2nd order polynomial feature of the equation implies that it can have two solutions- real or complex. Mathematically, quadratic equation can be shown in (3).

$$ax^2 + bx + c = 0, \tag{3}$$

By completing the square, one can easily determine the roots of variable x using (4).

$$x^2 + \frac{b}{a}x = -\frac{c}{a} \tag{4}$$

$$(x + \frac{b}{2a})^2 = -\frac{c}{a} + \frac{b^2}{4a^2} = \frac{b^2-4ac}{4a^2} \tag{5}$$

$$x + \frac{b}{2a} = \frac{\pm\sqrt{b^2-4ac}}{2a} \tag{6}$$

The formula obtained from (4) is called Quadratic formula" which is shown in (7)

$$x= \frac{-b\pm\sqrt{b^2-4ac}}{2a} \tag{7}$$

Solutions for (7) were found in Egypt [12]. The Greeks approached this equation by using geometric methods. Several Indian and Persian mathematicians have also tried to formulate rules to solve the equation. The basic purpose of the quadratic equation is to formulate a design for any object that may have curved surfaces, particularly spheres, parabolas, circles, ellipses etc. In the next section work carried out in the area of cryptography are discussed.

## 3. LITERATURE WORK

A considerable amount of literature was published in the field of Image encryption and Pell's equation. Following survey summarizes different researchers contributed in the field of cryptography. Ajib Susanto et.al. was proposed an image encryption technique containing 3 layers of encryption, which basically aims to secure images against statistical and differential attacks [13]. A. Rabie et.al. was introduced a method for encryption/decryption data by using the nature of FRFT in signals analysis, based on multi-order Fractional Fourier Transform has been introduced. The key is formed by combination of order of Fractional Fourier Transform [14]. Israa Al Barazanchi et.al. developed an enhanced RSA approach to make the encryption key more secure in the cryptographic applications [15].

Edward J Barbeau discusses the cubic analogue of Pell's equation. As he analyses a greater-degree form of the equation, it is obvious that the ideal choice is: $x^3 - dy^3 = k$. Barbeau's work suggests the equation: $x^3 + cy^3 + c^2z^2 - 3cxyz = k$ and analyses its compatibility with the quadratic case [16]. In paper [17], authors note that a Pell's equation of degree 2 can have a fundamental solution and also highlight that in a few scenarios where the equation is raised to the degree of 4 or 6, their solutions are extensions of solutions obtained from a lower degree equation. Raghunandan, K. R. et al. showed cubic power of pell's equations used to generate the keys using public key infrastructure is given and the results shown that the encryption system is secure from trial division, factorization attack [18]. A. Dubickas and J. Steuding proposed a methodology based on simple logarithmic properties. The authors elaborate the polynomial analogue of the pattern of a series of solutions of Pell's equation in numbers using generalization of Chebyshev polynomials and its corresponding trees [19]. T. Truong and J. Hedberggymnasiet approached Pell's equation as a concept in number theory that can be addressed as an open problem. The methodology suggests that the solutions generated are similar to the Pell's quadratic equation with certain exceptions. Through reviews and computational researches, the paper demonstrates that the equation serves its purpose in cryptography and approximation theory [20].

In paper [21] Raghunandan et.al. introduce the concept of fake modulus and fake public key exponent in enhanced RSA which can be proved secure from integer factorization attack. Sattar B. Sadkhan et.al. proposed variants of RSA which is based on the usage of quadratic equations. In this approach he used the quadratic equation for generation of keys [22]. Farah, M.A.B et.al. proposed an optimization technique using hybrid chaotic map to improve the performance of encryption function based on diffusion and confusion properties [23]. Manish Kumar et.al. was proposed a new algorithm using Elliptic Curve Cryptography (ECC) for image security, which makes use of DNA encoding [24].

## 4. RESEARCH METHOD

Key generation using Cubic Pell's Quadratic case is explored and explained using Figure 1. The entire process is subdivided into 3 sub sections. First sub section focuses on how the keys are generated using Cubic Pell's equation is explained. In the second sub section shows how the information at the sender side will be encrypted. Third subsection explains how the decryption process taken place at beneficiary side is explored.

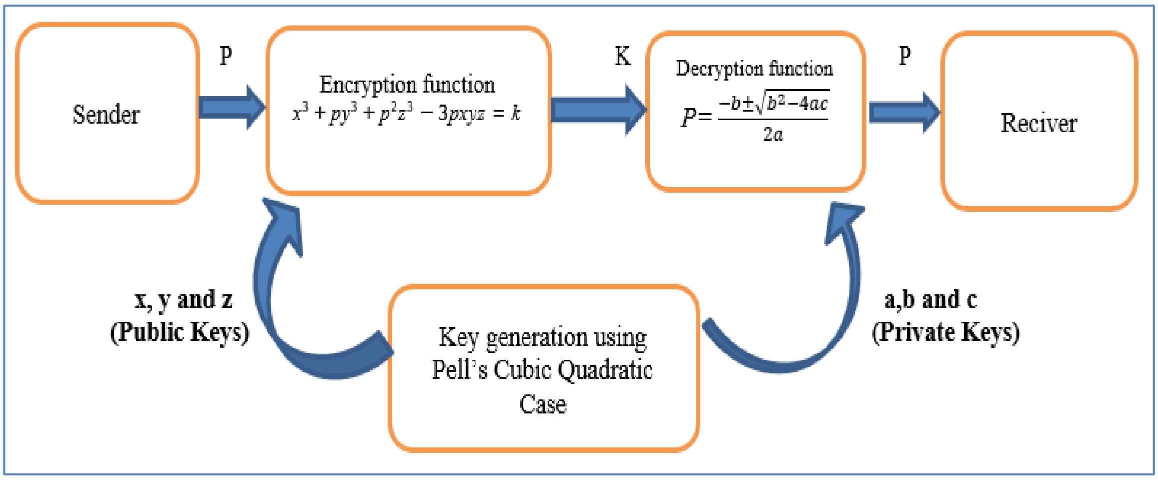


Figure 1. Key generation in public key cryptography using cubic pell's quadratic case for image encryption (P=Plain text, K=Cipher text)

### 4.1. Key generation

Pell's cubic equation written in Quadratic case using (8). Let p be the non perfect cube which is used to encrypt the information and *x, y* and *z* be the integer numbers which is used as the public keys

$$x^3 + py^3 + p^2z^2 - 3pxyz = 1 \tag{8}$$

Generalized form of (8) can also be written as (9) which can be used for encryption function

$$x^3 + py^3 + p^2z^3 - 3pxyz = k \tag{9}$$

By simplifying the quadratic case of (9) obtain the decryption keys *a,b* and *c* as follows

$$py^3 + p^2z^2 – 3pxyz = k - x^3 \tag{10}$$

$$p(y^3 + pz^3 - 3xyz) = \frac{k-x^3}{y^3+pz^3-3xyz} \tag{11}$$

After rewriting (10) & (11) we obtain,

$$z^3 p^2 + (y^3 - 3xyz)p + (x^3 - k) = 0 \tag{12}$$

The (12) is in the form of quadratic Equation (3) notation, from this obtain private key parameter *a* using (13), *b* obtained using (14) and *c* using (15).

$$a = z^3, \tag{13}$$

$$b = y^3 - 3xyz \tag{14}$$

$$c = x^3 - k \tag{15}$$

The values *x, y* and *z* were the keys used in the sender side along with the plain text to generate the cipher values. The keys *a, b* and *c* is shared to receiver to decrypt the original information (plain text) back from the cipher.

### 4.2. Encryption (sender side)

By using the Public key values *x,y* and *z* encrypt the data or information *p* using (9) and send the cipher or encrypted data *k* to the receiver through communication channel.

Example: Let *x=2, y=3* and *z=-1* which is used as Public keys, Let p=*4* be the plaintext which is to be encrypted. Computation of the cipher key *k* using (9) and obtained *172* as the cipher which is to be transmitted in the unsecured channel.

### 4.3. Decryption (reciever side)

In the receiver side by substituting the private keys i.e. *a,b* and *c* which is obtained from (13), (14) and (15) decrypt the original information back from the cipher text using (7)

Example: By receiving the private key values *a=-1,b=45* and *c=-164* apply the values to (7) obtain the plain text *k* =4 back.

In the following sections results are analysed and summarized and shows that Standard diviation and Entropy analysis of proposed scheme gives immunity to guess the encryption key and also it is difficult to break private keys using mathematical trics on public key using Diffrential analysis.

## 5. RESULTS AND DISCUSSION

In this section, explains different experimental results carried out to check the performance analysis of the proposed algorithm along with the comprehensive discussion about the experiment, computational difficulty and its analysis.

### 5.1. Experimental results

Experiment is carried out and tested by using 150 color images by taking different *x,y* and z key pairs. One of the sample Original image and cipher image is exposed in Figure 2 and Figure 3. It is apparent by the visual perception that no hint of plain image is accessible in the encrypted picture.

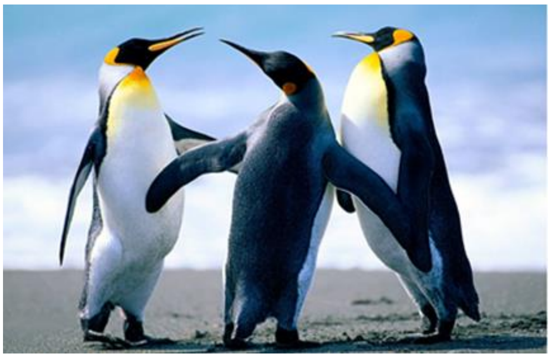


Figure 2. Original image (penguin)

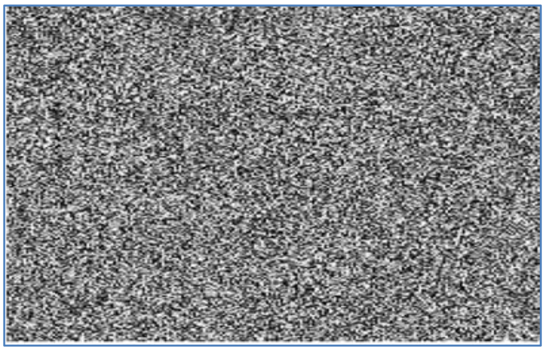


Figure 3. Encrypted (cipher) image

Histogram analysis refers to the distribution of intensity of pixels of the image, where each pixels have 256 intensity levels. The quantity of occurrences of pixels of plain image is plotted in y axis against the all estimations of the plain image pixel value in *x* axis which is shown in Figure 4. In Figure 5 the encrypted histogram obtained showcasing a flat histogram indicating almost all pixels are equiprobable and completely different than plain image, hence by the observations the proposed system is proved that leaking information to any intruder is not so easy through histogram-statistical attacks.

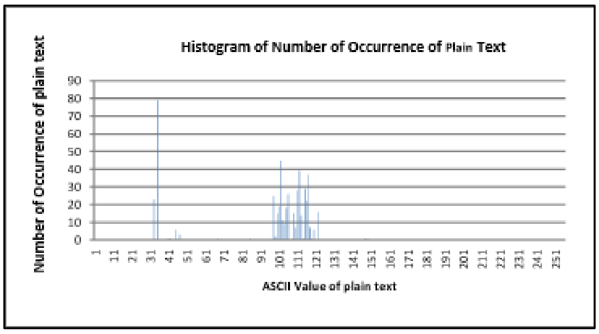


Figure 4. Histogram of plain image

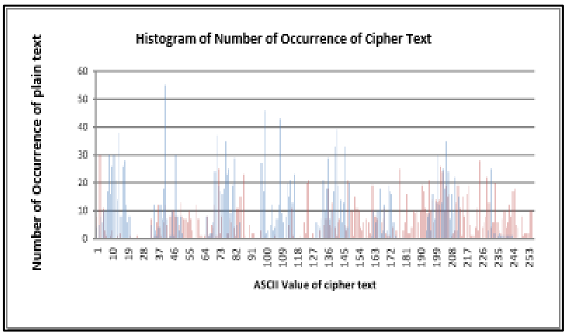


Figure 5. Histogram of encrypted image

## 5.2. Speed analysis

The conventional DES [25] and AES [26] encryption algorithms of Private Key framework work in Electronic Codebook mode, they are ineffectual against statistical attacks and chosen plain text attacks. Additionally, these two structures require no link between original and cipher images, and are defective even with differential attacks. To support and report the idea of proposed work in an auspicious way, standard "Penguin" image with different sizes are taken and the results are presented in the Table 1.

Table 1. Execution time in seconds

| Image | Aes | Des | Proposed method |
|---|---|---|---|
| Penguin(256×256) | 5.687 | 0.6397 | 0.0964 |
| Penguin (512×512) | 0.3475 | 7.4490 | 0.2744 |
| Penguin (1024×1024) | 1.1529 | 29.1139 | 0.2015 |

By comparing the results of proposed method with two Private Key algorithms AES and DES, it is observed that the time of execution used in the algorithm is justifiable with respect to speed.

## 5.3. Entropy analysis

Entropy is the measure of information involved by random source of information. Especially, if the source of information is redundant, then less information it contains [27]. The articulation of entropy is given by Shanon in (16). For an (*PC*) image of size (a,b), by posing (*t=ab, image value*) we get:

$$Entropy\ = H(PC)\frac{1}{t}\sum_{i=1}^{t} -p(i)\log_2\big(p(i)\big) \tag{16}$$

where PC= random image pixel values, t=occurance of pixel value.

The entropy values computed are graphically represented in Figure 6, where *X* axis represents the different samples of pixels taken into consideration and *Y* axis represents the enropy values for the same. The values of entropy of the proposed encrypted image 7.9898. It proves that the signal has got immunity to attack and is protected from entropy attack [28]. Hence it can be shown that the proposed work has achieved more strength with respect to its application in the field of cryptography.

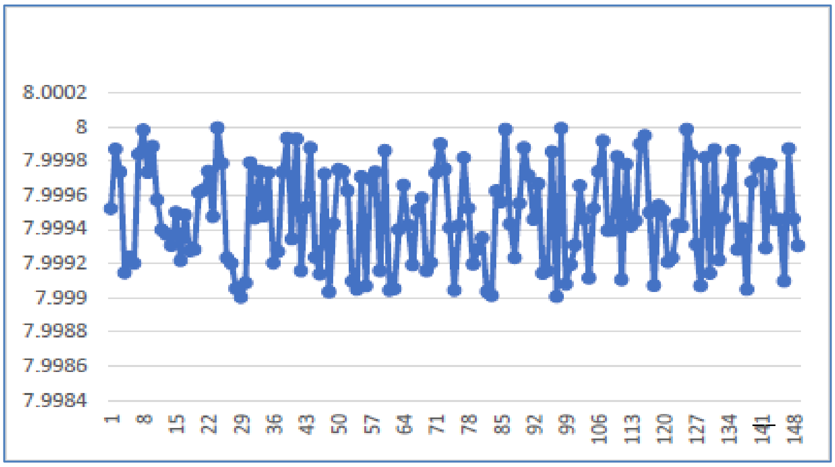


Figure 6. The entropy analysis of the proposed encrypted image

### 5.4. Asymmetry coefficient

The proportion of relationship between two binary factors is called as coefficient of skewness or Yule or asymmetry coefficient [29]. It is explained by the condition

$$S = \frac{(Q3-Q1)-(Q2-Q1)}{(Q3-Q1)} \quad = \frac{(Q3-2Q2+Q1)}{(Q3-Q1)} \tag{17}$$

Under these conditions S is the skewness and Q refers to Quartile, which defines the distribution of values, Yule has demonstrated that

*S=0 it has symmetry*
*S>0 Right Spreading or positive asymmetry*
*S<0 Left Spreading or negative asymmetry*

By using proposed method, using (17) obtained skewnesss = *0.33*which is parallel with the line of equality is above the axis of symmetry. Hence from the results its indication that mean values and the median values are too close, which makes difficult to judge individual values by intruders using different attack.

### 5.5. Correlation analysis

A system that performs comparision between two images to estimate the displacement of pixels in a single mode by comparing with one another is refered as Correlation. To provide imunity from any statistical attack, a standard cryptography image framework must remove correlations [30]. The expression used to find the correlation can be expressed using (18),

$$Correlation\ (\Upsilon) = \frac{cov(x,y)}{\sigma(y)\sigma(x)} \tag{18}$$

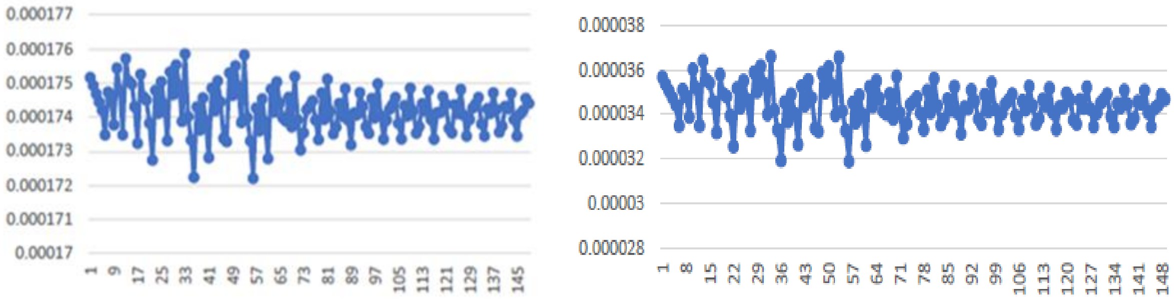
where, ϒ be the correlation coefficient, $cov(x, y)$ denotes covariance of variables *x* and *y*, *σ(x)* will be the standard deviation of *x*, and *σ(y)* be the standard deviation of *y*. The results obtained in the Table 2 guarantees high protection from correlation attack.

Table 2. Correlation coefficient analysis of original image and cipher image

| Directions | Original image | | | Cipher image | | |
|---|---|---|---|---|---|---|
| | Red | Green | Blue | Red | Green | Blue |
| Horizontal | 0.9448 | 0.9403 | 0.8773 | 0.0093 | 0.0012 | 0.0053 |
| Vertical | 0.9656 | 0.9696 | 0.9554 | 0.0082 | 0.0021 | 0.0083 |
| Diagonal | 0.9134 | 0.9115 | 0.8513 | 0.0016 | 0.0172 | 0.0053 |

### 5.5.1. Horizontal and vertical correlation

In Horizontal correlation analysis sequences are analysed horizontally where in vertical correlation sequences are analyzed vertically. Simulations performed on Plain image (Figure 1) and the obtained correlated values are represented graphically using Figure 7.



(a) (b)

Figure 7. Correlation of cipher image, (a) Horizontal, (b) Vertical

### 5.5.2. Diagonal correlation

Simulation results for the image gave the diagonal correlation as depicted in Figure 8. Results in the graph indicates that the enciphered results of the cipher images are correlates near to zero. This guarantees high protection from correlation attack.

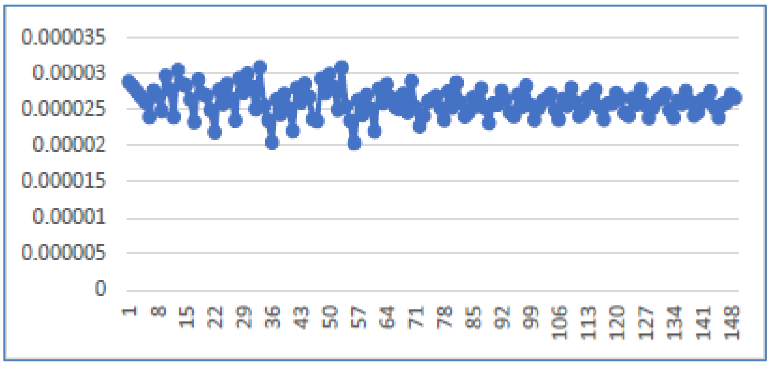


Figure 8. Diagonal correlation of cipher image

### 5.6. Differential analysis

Differential analysis is a metric used to check the resistence of the cipher in differential attack analysis. Generally, when intruder makes little changes on the original image (flipping one bit), observing the difference in the cipher image might help to locate applicable association with original and cipher image. Hence in such situation this differential attack is not an effective. Therefore, to evaluate the impact of pixel change on the enciphered image, Number of Pixel change Rate (NPCR) is given in (19)

$$NCPR = \left(\frac{1}{nm}\sum_{i,j=1}^{n,m} D(i,j)\right) \times 100 \tag{19}$$

$$with\ D(i,j) = 1\ if\ c_1(i,j) \neq c_2(i,j)\ and\ D(i,j) = 0\ if\ c_1(i,j) = c_2(i,j)$$

In the Figure 9, Y axis shows the NPCR calculation and X axis shows different imageof varied sizes. It clearly shows that every identified value is inside the confidence intermission [99.63 to 99.95]. This qualities of proposed method is significant enough to protect from known differential attacks [31].

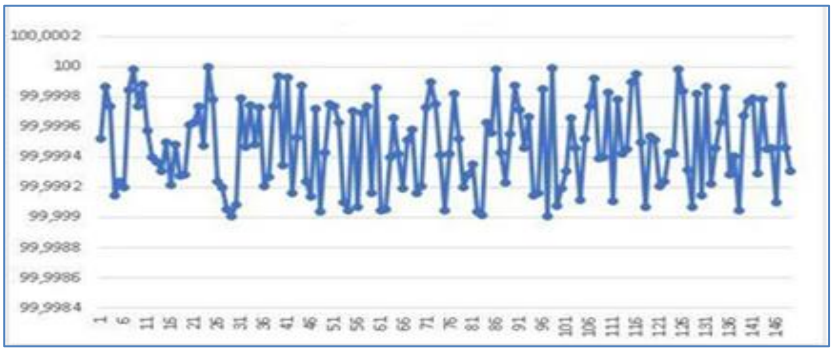


Figure 9. Number of pixel change rate (NPCR) of cipher images

### 5.7. Avalanche effect

It is a essential metric used in all purposes of cryptographic algorithms. It causes dynamically increasing significant changes as the information is spreading in the structure of the algorithm. Consequently, a piece or bit of the original image, obtaining huge rate of change in the encrypted image [32-34]. It is explained using (20)

$$Avalache\ Effect(AE) = \left(\frac{\sum_i bit\ change}{\sum_i bit\ total}\right) \times 100 \tag{20}$$

Figure 10 shows a small change in the original image leads to a tremendous change in the cipher text, which in turn makes it hard to decrypt the image and obtain the original image back.

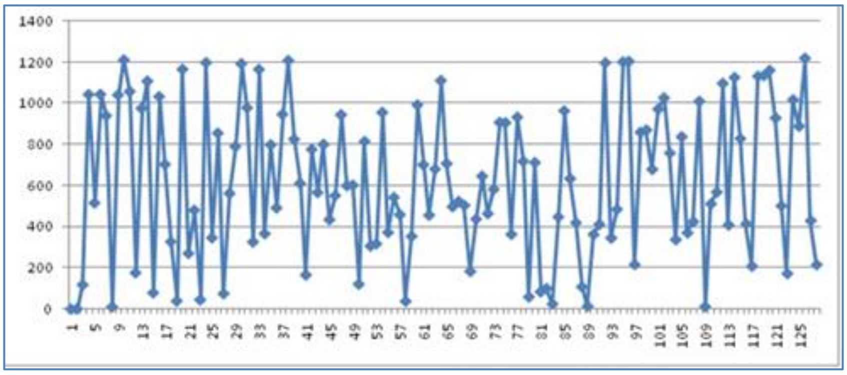


Figure 10. Avalanche effect of proposed scheme

## 6. CONCLUSION

By addressing security as primary objective, proposed method made an improvement in the field of cryptography by introducing a novel technique. With strong evidences showcased in the results of proposed method which is built on the strong foundations of quadratic equations and Pell's equation proved that the metgod is immune to the vulnerabilities of existing cipher systems. To measure the encryption quality and robustness, rigorous analysis and experiments conducted on the system which includes entropy analysis, correlational analysis, differential analysis and avalanche effect. Outcome of the experiments ensures that this new security scheme has solid security, high robustness and can be constructed with ease and be effectively used for light weight applications.

## REFERENCES

[1] L. D. Singh and K. M. Singh, "Implementation of text encryption using elliptic curve cryptography," *Procedia Computer Science,* vol. 54, pp. 73-82, 2015.

[2] Raghunandan K. R., et al., "Comparative Analysis of Encryption and Decryption Techniques Using Mersenne Prime Numbers and Phony Modulus to Avoid Factorization Attack of RSA," *Proceedings of the International Conference on Advanced Mechatronics Systems*, Katsugu, Japan, pp. 152-157, 2019.

[3] J. I. Ahmad, et al., "Analysis Review on Public Key Cryptography Algorithms," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 12, no. 2, pp. 447-454, 2018.

[4] G. Alvarez, et al., "Analysis of security problems in a medical image encryption system," *Computers in Biology and Medicine*, vol. 37, no. 3, pp. 424-442, 2007.

[5] F. T. B. Muhaya, "Cryptanalysis and security enhancement of Zhu's authentication scheme for Telecare medicine information system," *Security and Communication Networks,* vol. 8, no. 2, pp. 149-158, 2015.

[6] L. Chen and S. Wang, "Differential cryptanalysis of a medical image cryptosystem with multiple rounds," *Computers in Biology and Medicine,* vol. 65, pp. 69-75, 2015.

[7] S. Nikitin, "Euler-Fermat algorithm and some of its applications," Arizona State University, pp. 1-15, 2018.

[8] F. Patte, "The resolution of Diophantine equations according to Bhāskara and a justification of the cakravāla by Kṛṣṇadaivajña," *Mathematics in Ancient Times,* Kozhikode, India, vol. 32, no. 1-2, pp. 73-105, 2010.

[9] M. Acewicz and K. Pąk, "Pell's Equation," *Formalized Mathematics*, vol. 25, no. 3, pp. 197-204, 2017.

[10] H. W. Lenstra, "Solving the Pell equation," *Algorithmic Number Theory*, vol. 44, pp. 1-24, 2008.

[11] D. M. Burton, "Elementary Number Theory," New York, McGraw-Hill, 2007.

[12] D. E. Smith, "History of Mathematics," New York, Dover Publications, vol. 1, 1958.

[13] A. Susanto, et al., "Triple layer image security using bit-shift, chaos, and stream encryption," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 3, pp. 980-987, 2020.

[14] A. Rabie, et al., "Data encryption based on multi-order FRFT, and FPGA implementation of des algorithm," *International Journal of Reconfigurable and Embedded Systems (IJRES),* vol. 9, no. 2, pp. 141-152, 2020.

[15] I. Al-Barazanchi, et al., "Modified RSA-based algorithm: a double secure approach," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 17, no. 6, pp. 2818-2825, 2019.

[16] E. J. Barbeau, "Pell's Equation," Problem Books in Mathematics, Springer, pp. 1-212, 2003.

[17] E. J. Barbeau, "The Cubic Analogue of Pell's Equation," in Pell's Equation, Problem Books in Mathematics, Springer, pp. 92-112, 2003.

[18] Raghunandan K. R., et al., "Key generation and security analysis of text cryptography using cubic power of Pell's equation," *2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT),* pp. 1496-1500, 2017.

[19] A. Dubickas and J. Steuding, "The polynomial Pell equation," *Elemente der Mathematik,* vol. 59, no. 4, pp. 133-143, 2004.

[20] T. Truong, "Cubic Pell Equation," Johannes Hedberggymnasiet, Project Course, 2012.

[21] K. R. Raghunandhan, S. Shetty, G. Aithal and N. Rakshith, "Enhanced RSA Algorithm using Fake Modulus and Fake Public Key Exponent," *2018 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT),* Msyuru, India, 2018, pp. 755-759, doi: 10.1109/ICEECCOT43722.2018.9001351.

[22] S. B. S. Al Maliky and L. H. Al-Siwidi, "RSA-Public Key Cryptosystems Based on Quadratic Equations in Finite Field," *Multidisciplinary Perspectives in Cryptology and Information Security,* IGI Global, pp. 238-258, 2014.

[23] M. A. B. Farah, et al., "An image encryption scheme based on a new hybrid chaotic map and optimized substitution box," *Nonlinear Dynamics*, vol. 99, pp. 3041-3064, 2020.

[24] M. Kumar, et al., "A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie-Hellman cryptography," *Signal Processing,* vol. 125, pp. 187-202, 2016.

[25] A. Houas, et al., "A novel binary image encryption algorithm based on diffuse representation," *Engineering Science and Technology, an International Journal*, vol. 19, no. 4, pp. 1887-1894, 2016.

[26] D. C. Mishra, et al., "Security of RGB image data by affine hill cipher overSLn (Fq) and Mn (Fq) domains with Arnoldtransform," *Optik*, vol. 126, no. 23, pp. 3812-3822, 2015.

[27] R. K. Niven, et al., "Maximum Entropy Analysis of Flow Networks: Theoretical Foundation and Applications," *Entropy*, vol. 21, no. 8, pp. 776-795, 2019.

[28] A. J. Newell, et al., "Entropy attacks and countermeasures in wireless network coding," *Proceedings of the 5th ACM conference on Security and Privacy in Wireless and Mobile Networks*, pp. 185-196, 2012.

[29] Y. Shuangyuan, et al., "An asymmetric image encryption based on matrix transformation," *IEEE International Symposium on Communications and Information Technology,* vol. 1, pp. 66-69, 2004.

[30] N. J. Gogtay and U. M. Thatte, "Principles of Correlation Analysis," *The Journal of the Association of Physicians of India,* vol. 65, no. 3, pp. 78-81, 2017.

[31] E. Biham and A. Shamir, "Differential Cryptanalysis of the Data Encryption Standard," Springer, 1993.

[32] M. Ukrop and P. Svenda, "Avalanche Effect in Improperly Initialized CAESAR Candidates," *Electronic Proceedings in Theoretical Computer Science,* vol. 233, pp. 72-81, 2016.

[33] Raghunandan K. R., et al., "Secure RSA Variant System to Avoid Factorization Attack using Phony Modules and Phony Public Key Exponent," *International Journal of Innovative Technology and Exploring Engineering (IJITEE),* vol. 8, no. 9, pp. 1065-1070, Jul 2019.

[34] Y. Rajput and A. K. Gulve, "A Comparative Performance Analysis of an Image Encryption Technique using Extended Hill Cipher," International Journal of Computer Applications, vol. 95, no. 4, pp. 16-20, Jun 2014.

## BIOGRAPHIES OF AUTHORS

**Raghunandan K R** working as Assistant professor in the Department Of Computer Science and Engineering, NMAM Institute Of Technology,Nitte. He is pursuing his Ph.D from Visvesaraya Technological University in the field of Public key Cryptography. He has published around 12 Research Papers in different international journals and conferences. The research ares of interest are Cryptography, Bloch Chain, Parallel Processing.

**Dr. Ganesh Aithal,** working as Professor & Vice Principal at Shri Madhwa Vadiraja Institute of Technology and Management, Banatakal, Udupi Karnataka – India. He is currently guiding 4 research scholars. The Research areas of interest are Cryptography and Securities -Random Number Generator, Stream Cipher System, Parallel Processing in the area of Cryptography, Public Key Cryptographic System and Securities in the area of Sensor Networks.

**Dr. Surendra Shetty**, Professor & Head had been awarded his doctoral degree for his research work “Audio Data Mining Using Machine Learning Techniques” in 2013 from university of Mangalore. He has published more than 25 research papers in different international journals and conferences. He is currently guiding six research scholars. Dr. Surendra Shetty authored two book chapters in different publications entitled “Machine Learning Approach for Carnatic Music Analysis” and “Applications of Unsupervised Techniques for Clustering of Audio Data”. He has received research grant of 20 lakhs from VGST (GoK) for carrying out research on “Automatic Natural Language Processing and Speech Disorder Problems in Kannada Language”. The Research areas of interest are Cryptography, Data mining, Pattern Recognition, Speech Recognition, MIS, Software Engineering and Testing.

**Bhavya K**, working as Assistant Professor in the Department of Mathematics, NMAM Institute Of Technology,Nitte. The Research areas of interest are Number theory, Graph theory, Cryptography.