New approach to Generate, Re-Generate, Encode, and Compress 3D structures using polynomial equations

Jimut Bahan Pal¹, Asoke Nath²

¹,²Department of Computer Science, St. Xavier’s College (Autonomous), 30 Park Street, Kolkata, India

*Corresponding Author: asokejoy1@gmail.com, Tel.: +033-22876035

Available online at: www.ijcseonline.org

Accepted: 18/Dec/2018, Published: 31/Dec/2018

Abstract— Almost every 3D objects can be represented with the help of a set of equations. When 3D objects are converted to text in terms of equations, any standard cryptographic techniques can be applied to encrypt it. This method is useful to hide classified military secrets, as we compress it to a large amount in the form of text, yet it can be regenerated in mathmod software, after decrypting it using the key. In this study, we propose a new way to formulate polynomial equation of any objects in context by fitting it using brute force techniques. We find that the complexity of the algorithm is too high to be achieved in practical scenarios, which encourages more efficient work in this new field.

Keywords— Compression, Cryptographic techniques, Generation, 3D, and Polynomial equations.

I. INTRODUCTION

Almost everything we see in this mundane world can be represented using complex polynomial equations. Aren’t they? Most of the simple objects can be represented directly. The objects in 2D can be easily represented using a set of equations and defining the range and domain of x, and y values as shown in Fig. 1, and Fig. 2.

Fig. 1: A 2D representation of DeLauro [1]

We can represent objects in 3D too. Let’s take an example of a simple heart in 3D as shown in Fig. 3, and look at the relevant equation carefully. It represents a polynomial equation of 6 degrees.

Fig. 2: A 2D representation of Minion [1]

Let’s talk about modelling an object in any standard animation software. There are several modelling softwares, like CAD which has.stl extension. It stores mainly the vertices. Another one being 3DS, now owned by Autodesk Maya. It stores data in the form of binary chunk, similar to XML DOM tree with a .3ds extension. Flimbox or (.fbx) files are also modelled using Autodesk. This can be formatted to represent high quality models with textures.

We are working with vertices, edges and faces of the object to design the model. Now, what is a face? A face is a 2D side of any 3D object. For example, a cube may have 6 faces. It is always necessary to have edges more than 2, i.e., 3 edges to have one face. Now, if we draw a pentagon in a white paper...
sheet, it will have one face but should have 5 edges, likewise
if we draw a triangle it will have 3 edges and one face, and
so on. Similarly, when we work with any modeling software,
we will work with face and edges and make necessary
changes like a sculptor to change the shape and nature of the
object in context. More the number of faces, vertices or
edges, more the size of the object. Now, what the .obj
(object) files are storing in it? It generally stores the position
of edges, vertices in an optimized binary format, with some
meta-data about the software, time etc. We can also easily
analyze the object file by opening it in any text editor, like
vim for opening large files in short time. So, what happens in
general case is that those models which are made through the
general animation or modeling software are large in size. It
takes much memory to store. Here, we presented a new
method to compress the existing models, to generate models
with the help of equations.

Here we have encrypted some simple objects with the help of
equations and represented it with any standard 3D modelling
software. Firstly we have shown that even complex models
can be represented with the help of equations, then we have
encrypted a simple heart shaped structure with the help of
software to text equations. We have then encrypted the same
with the help of the famous AES algorithm, then decrypted it
to show that it is lose less compression. We have also shown
other standard encryption techniques and shown why we
prefer AES algorithm, we have also developed a brute force
algorithm to make complex equations, match it and select
the equation of best fit. Further we have analyzed the complexity
of the algorithm to find any general structure, and realized
that it is too high to be achieved in practical scenarios, so it
will encourage more work in this new field to find other
methods which will form lose less compression to existing
3D structures to equations. We can use B-spline, T-spline
methods, but they may result in loss of 3D data and
precision, so some other methods should be devised which
will be lose less and be feasible in low hardware resources.

II. RELATED WORK

Innumerable literatures are available in the field of computer
graphics, simulation, visualization and real time analysis of
pictures to generate, regenerate and fill missing parts using
machine learning technologies and mathematical models.
Some of the works by different researchers are brought to
context which includes fitting of polynomial to take pictures
of palm for a very strong biometric security. Furthermore,
there has been study of regeneration of missing and broken
vertices, creating 3D shapes and structures of a 2D image of
an object in context. Researchers found better methods to
help solving real time problems like determining the
acceleration due to gravity of an irregular shape asteroid.

The property of interpolation, Euclidean, affine invariants
and their ability to represent complex objects makes the
implicit polynomials represent useful object and data in
computer vision [3, 4]. Blane et al. [3] studied and improved
the former methods to model the fingers by using implicit
polynomial fit strategy, resulting in identifying fingers using
biometric methods. They tested it till 5th degree with
satisfying results, obviously the higher the degree of
polynomial higher is the precision, formulating 3L algorithm,
which provides a fast solution to its counterparts, with a
better repeatability and numerical stability. It can easily fit
polynomial of high degree such as 14th to 18th.

Cost and time could be significantly reduced by procedurally
generating the content, leveraging the creativity of the
designers, programmers and artists. Quiroz et al. [5] used
genetic algorithm to procedurally generate vertex shades of
3D models in web applications. The main problem in
robotics, virtual reality, augmented reality, and computer
graphics is to determine the proximity relationships between
3D objects cluttered in an environment in real time. The path
planners in robotics [6] computes a dynamically feasible trajectory from starting position to goal, while avoiding obstacles. In game engines, VR, real time simulations, and all objects in a scene shall interact to respond and emulate physics in the real world. Ahmadi et al. [6] studied the problems of spatial analysis of 3D environment using sublevels of polynomials, and performing complex mathematical operations on cloud of data points, to get the knowledge of geometry and surroundings.

Irregular shapes of asteroids may lower the efficiency of calculating the gravitational field that is experienced by it. Hu et al. [7] studied and proposed a method to use Chebyshev polynomial interpolation to adapt and divide the space near the asteroid along spherical co-ordinates. Then it represents gravitational acceleration in each cell. This increases the efficiency in measuring gravitational force accurately. A face recognition method presented by Komorowski et al. [8] is based on sequencing images, which is easy to implement. The use of laser scanners may be expensive, large and may cause damage to human organs. They reconstructed face shape using multi view stereo methods and motion of the object. Since it is based on images only, it is easy to use, and do not require any face model. Human perceive objects through semantic reasoning, can forecast about the geometry as well as the 3D shape of the object by limited 2D information. This helps us to interact with the objects easily. Mandikal [9] et al. further studied the reconstruction of image through 3D cloud from a single input image. They showed that when they trained task jointly, it yields better results than training each task individually. Using ShapeNet dataset, they improved results in reconstruction as well as segmentation of objects. A 3D mesh animation of sequences was synthesized with long short term memory (LSTM) blocks and mesh based Convolutional Neural Networks (CNNs) [10]. A Polyharmonic Radial Basis functions (RBF) could be used to reconstruct smooth manifold surfaces from point based cloud data and incomplete meshes could be repaired too as studied by Carr et al. [11].

To enhance navigation, visualization, urban planning of historic and touristic objects, 3D building models becomes important during the past years [12]. It helps to understand scenarios that make complex decisions. Gross et al. studied 3D modeling of buildings from maps by semi-automatic processing of laser scanner elevation of the building using aerial imagery. Kholgade et al. presented a method [13], which can perform full range of 3D operations such as scaling, translation, rotation etc. to an object in photograph. It is better than the 2D conventional operation that gives a realistic effect. It takes input from a 2D image and uses publicly available dataset of model to complete the unseen part of the 2D image in context.

III. METHODOLOGY

We can represent any structure in the form of equations. We used mathmod software [14] to represent any objects using equations. The objects as shown in Fig. 5 represents an arena. The objects can be represented with a set of equations:

\[
  \begin{align*}
    27 < & 0 & \text{abs}(x < (10), \text{ThickIsoExterior}(x, y, z, t), 1) \\
    \text{With additional set of functions:} \\
    \text{Scherk} = & \text{Sinh}(x) \times \text{Sinh}(y) \times 4 \times \text{Sinh}(z) \\
    \text{Scherk}2 = & \text{Sinh}(x, \text{Sqrt}(y + z) - (16), N \times \text{atan2}(z, y), t) \\
    \text{Thickness}2 = & (0, 6)
  \end{align*}
\]

\[
  \begin{align*}
    \text{IsoExterior} = & \text{Scherk2}(x, y, z, t) \\
    \text{DFx2} = & (\text{IsoExterior}(x, y, z, t) - \text{IsoExterior}(x + cy, y, z, t) \times cy) \\
    \text{DFy2} = & (\text{IsoExterior}(x, y, z, t) - \text{IsoExterior}(x, y + cy, z, t) \times cy) \\
    \text{Dfz2} = & (\text{IsoExterior}(x, y, z, t) - \text{IsoExterior}(x, y, z + cz, t) \times cz) \\
    \text{Rapport2} = & (\text{Sqrt}(\text{DFx2}(x, y, z, t) - \text{DFy2}(x, y, z, t) + \text{DFy2}(x, y, z, t)) \times \text{Dfz2}(x, y, z, t)) \\
    \text{Iso3} = & (\text{IsoExterior}(x - \text{DFx2}(x, y, z, t) \times \text{Thickness2}(x, y, z, t) \times \text{Rapport2}(x, y, z, t), y + \text{DFy2}(x, y, z, t) \times \text{Thickness2}(x, y, z, t) \times \text{Rapport2}(x, y, z, t), z + \text{DFz2}(x, y, z, t) \times \text{Thickness2}(x, y, z, t) \times \text{Rapport2}(x, y, z, t), t)) \\
    \text{ThickIsoExterior} = & (\text{Iso2}(x, y, z, t) \times \text{Iso3}(x, y, z, t))
  \end{align*}
\]

A range of x, y, and z domain values:

\[
  \begin{align*}
    x = & -10.1 \text{ to } 10.1 \\
    y = & -28 \text{ to } 28 \\
    z = & -28 \text{ to } 28
  \end{align*}
\]

So, if we take this model and sculpt any animation or modelling software, then it would take more than 10 Mb of space depending on the number of vertex and faces to a large extent, but in representing this in terms of equations in text file it takes a less memory to store some bytes of equations. Similarly, we can represent all the 3D objects in Fig. 4, Fig. 5, Fig. 6, Fig. 7, Fig. 8, Fig. 9, Fig. 10, Fig. 11, and Fig. 12 using a set of equations.
Similarly, the broken vase shown in Fig. 9 can be represented using the following set of equations:

\[ \text{isoTransform}_2(x,y,z,t) \ast \text{isoTransform}_6(x,y,z,t) \]

With an additional set of functions:

\[ \text{Angle1} = \frac{\text{atan2}(\sqrt{x^2+y^2}, (-z+cx))}{(z+cx)} \]

\[ \text{Angle2} = \frac{\text{atan2}(x, (y+cx))}{(y+cx)} \]

\[ \text{CarvinCondition} = \frac{\text{abs}(z-1) - 0.8 \times \text{cos}(18 \times \text{Angle2}(x,y,z,t/\pi))}{10.3 - 0.3 \times \text{cos}(18 \times \text{Angle2}(x,y,z,t/\pi+\pi/4))} < 0.5 \]

\[ \text{Iso} = \text{cos}(x) \times \text{sin}(y) + \text{cos}(y) \times \text{sin}(z) + \text{cos}(z) \times \text{sin}(x) \]

\[ \text{Torus} = \left( \sqrt{x^2+y^2} - 3 \right)^2 + z^2 - 1 \]

\[ \text{Bottom} = (x^3 + y^3 + z^3 - 1) \]

\[ \text{Iso} = \text{cos}(x) \times \text{sin}(y) + \text{cos}(y) \times \text{sin}(z) + \text{cos}(z) \times \text{sin}(x) \]

\[ \text{Dfx} = \left( \text{Iso}(x,y,z,t) - \text{Iso}(x+cx,y,z,t) \right) / cx \]

\[ \text{Dfy} = \left( \text{Iso}(x,y,z,t) - \text{Iso}(x,y+cy,z,t) \right) / cy \]

\[ \text{Dfz} = \left( \text{Iso}(x,y,z,t) - \text{Iso}(x,y,z+cz,t) \right) / cz \]

\[ \text{Rapport} = \sqrt{\text{Dfx}(x,y,z,t)^2 + \text{Dfy}(x,y,z,t)^2 + \text{Dfz}(x,y,z,t)^2} \]

\[ \text{Iso4} = \text{Iso}(x+t \ast \text{Dfx}(x,y,z,t) \ast \text{Thickness4}/\text{Rapport}(x,y,z,t), y+t \ast \text{Dfy}(x,y,z,t) \ast \text{Thickness4}/\text{Rapport}(x,y,z,t), z+t \ast \text{Dfz}(x,y,z,t) \ast \text{Thickness4}/\text{Rapport}(x,y,z,t), t) \]

\[ \text{ThinIso4} = \text{Thin}(\text{Iso4}(x,y,z,t)) \]

\[ \text{isoTransform}_2 = \text{if}(\text{CarvinCondition}(x,y,z,t) = 0, \text{ThinIsoExterior}(x,y,z,t)) \]

\[ \text{Iso6} = \text{Iso}(x+t \ast \text{Dfx}(x,y,z,t) \ast \text{Thickness6}/\text{Rapport}(x,y,z,t), y+t \ast \text{Dfy}(x,y,z,t) \ast \text{Thickness6}/\text{Rapport}(x,y,z,t), z+t \ast \text{Dfz}(x,y,z,t) \ast \text{Thickness6}/\text{Rapport}(x,y,z,t), t) \]

\[ \text{isoTransform}_6 = \text{if}(\text{CarvinCondition}(x,y,z,t) = 0, \text{ThinIso6}(x,y,z,t) \& \text{ThinIsoExterior}(x,y,z,t)) \]

With x, y, and z domain being:

\[ x = -3.5 \text{ to } 3.5 \]
\[ y = -3.5 \text{ to } 3.5 \]
\[ z = -5 \text{ to } 4.5 \]

Above two examples simplify the complex structures that may be represented using a set of equations. In this paper we studied the example of a heart, and compared the sizes when it represents terms of equations using plain text, encrypt with AES algorithm and decrypt it using the same to regenerate it using the text. We have also presented here an algorithm to brute force using a model to a complex polynomial equation. We will also discuss the complexity of the model, and its future scope in results and discussion to improving it to a large extent.
A. Generating the model from the equation

The equation of heart is 
\[
(x^2 + \frac{9}{4}y^2 + z^2 - 1)^3 - (x^2)(z^3) - (9/200)(y^2)(z^3),
\]
we can use this equation to represent it in math-mods as shown in Fig. 13. The equation will take about 75 bytes in plain text. When we sculpt a heart model using Maya, a standard modelling and animation software, its size is increased to 476 KB as shown in Fig. 14. We can thus see that to represent it using Maya, the size has increased to about 6499 times. The only problem with our method is that it doesn’t represent a smooth surface but it can be achieved with higher degree of polynomial equations.

Hence, the model can be represented using a polynomial equation, by compressing it to a large extent.

B. Encrypting the equation

Once we converted the model to equation, i.e., in the text from, we can apply it to any standard encryption algorithm for encryption. Some of the standard encryption algorithms [15] are:

1. **Triple Des**: It was designed to replace the Data Encryption Standard (DES) Algorithm. It uses three individual keys of 56 bits each of which adds up to 186 bits. It still serves as encryption algorithm for financial services and other industries.

2. **RSA**: It is an asymmetric algorithm as it has pair of keys. It is the standard for encrypting data sent over the internet, and is a public-key encryption algorithm.
3. **Blowfish**: It replaced DES algorithm. It manages to split messages into blocks of 64 bits and then encrypts them individually.

4. **Twofish**: It is the successor of blowfish. The key can be up to 256 bits in length, and only one key is required as it is symmetric.

5. **Rijndael or Advanced Encryption Standard (AES)**: It is trusted as a standard of encryption [16] by the US government and other organizations. It is extremely efficient in encryption. It has 128-bit form keys (Fig. 15). It also uses keys of length 192 and 256 bits for heavy duty encryption purposes. It is designed to have only single whole byte operations.

We have used the AES or Rijndael encryption standard for encrypting our equation, 
\[
(x^2 + (9/4)y^2 + z^2 - 1)^{3/2} - (x^2 + (9/200)y^2 + z^2)^3.
\]
After encryption of the equation, we get text as shown in Fig. 16.

Till now we successfully encrypted the text using Rijndael 256-bit encryption with a key value of 4. In this study we used the online tool for applying this cryptographic encryption [17]. The size of the binary format of the encrypted downloaded text was 96 bytes, which is still small compared to the rendered model in Maya. Now, we want to decrypt the encryption using the same key. On decrypting we get back the plain text in the form of equation as shown in Fig. 17.

From the above investigation we can find that this form of storing information or model can be very useful for classified military objects. Now decrypting we get the text that can easily generate the model by passing it in math-mod as shown in Fig. 13.

**C. New brute force Algorithm to encrypt already existing models**

We proposed here a new algorithm which can brute force and try all possible combination to match the polynomial.

\[
\text{General algorithm for brute force} = (1 + f(x) + f(y) + f(z)) \sum_{i=0}^{n} x^i \sum_{j=0}^{m} y^j \sum_{k=0}^{p} z^k\]

Where,
\[
f(x) = \sin(x) + \cos(x) + e^x + \log(x) + \ldots + k \text{ terms},
\]
\[
f(y) = \sin(y) + \cos(y) + e^y + \log(y) + \ldots + k \text{ terms},\]
\[
f(z) = \sin(z) + \cos(z) + e^z + \log(z) + \ldots + k \text{ terms}
\]

Where \( f \) is a function that have all the trigonometric, logarithmic and exponential functions available. We can
increase the no. of components in as much as possible, but the complexity will increase too.

It will generate all possible combination of equations starting from one, and match the model generated, deduct the error and try the next possible iteration, by which it will be more accurate. Though, the complexity will be high, but we can reduce to a great extent after getting minimum error for a certain polynomial equation. A simulation is shown in Fig. 18, as a possible behavior of the equation as a part of the model.

The above object is easy, simple or small, but when the object is complex, we can break the model into parts and then fit the general brute force equation as shown in Fig. 19.

The model is first broken into parts of equal sizes in order, and then it is tested on equations which give the perfect fit. Then it is arranged and stored in the same fashion as it is broken. The sequence numbers are given. Then it is encrypted and stored, successfully reducing the size. After that it is decrypted with the help of key and it is generated in the same sequence as it was encrypted.

In this way, we can encrypt existing models. We can even encrypt real life pictures, by turning it into models, and then using this brute force polynomial generation algorithm to match the model. After that we can use any standard encryption technique to successfully encrypt it.

IV. RESULTS AND DISCUSSION

We found that everything in this world can be represented in terms of polynomial equations. We also used the math-mod software to successfully generate a heart and encrypt it using standard encryption techniques, resulting in higher compression as compared to its Maya’s counterpart. We also proposed an algorithm to generate all possible combinations of polynomial equations and then match it, and selecting the equation for good fit. In this way we can encrypt existing models. We can even encrypt real life objects, initially making a model of it through standard techniques and fitting the equations.

Let’s take an example of the equation for 1 degree polynomial (i.e., n = 1) and then testing it on only, f(x) = sin(x), f(y) = sin(y), and sin (z) i.e., k = 1. So, the equation becomes:

\[
(1+\sin(x)+\sin(y)+\sin(z)).(1+x).(1+y).(1+z)
\]

Now, we will take constants, \(C_1, C_2, C_3, ..., C_{(k+3)(n+1)}\), the final equation becomes:

\[
C_1.1 + C_2.x + C_3.y + C_4.z + C_5.x.y + C_6.z.x + C_7.z.y + C_8.x.y.z + C_9.y.z + C_{10}.y.z + C_{11}.y.z + C_{12}.z.sin(x) + C_{13}.x.y.sin(x) + C_{14}.z.x.sin(x) + C_{15}.z.y.sin(x) + C_{16}.y.z.sin(x) + C_{17}.sin(y) + C_{18}.x.sin(y) + C_{19}.y.sin(y) + C_{20}.y.sin(y) + C_{21}.y.sin(y) + C_{22}.x.sin(y) + C_{23}.z.sin(y) + C_{24}.x.y.sin(y) + C_{25}.sin(z) + C_{26}.x.sin(z) + C_{27}.y.sin(z) + C_{28}.z.sin(z) + C_{29}.y.z.sin(z) + C_{30}.z.x.sin(z) + C_{31}.z.y.sin(z) + C_{32}.x.y.z.sin(z)
\]

After multiplying different variables with each component, we will set a boundary value for tweaking those variables which will be constant for a particular set of equation. For this equation, let it be 10. For each component it will have 10 values, and there are total 32 components, which means that for the total number of equations it will calculate is \(10^{32}\). The computing complexity will be tremendous, and it could be achieved with the help of a super computer. The computing
complexity for this algorithm is shown in Fig. 20, which means it is almost practically impossible to test this in a normal computer, we can also skip some of the values and then it will be a little bit smaller, for example we can take even values only. After taking the even values, the value of $c$ will be 5 and the number of equations formed will be $5^2$.

If this is too much, we can ignore more of these equation by ignoring similar values, but this will take more time and resource in a normal computer.

V. CONCLUSION AND FUTURE SCOPE

Above findings show that any model can be represented in terms of equations, i.e., texts form. Which means that they can be encrypted using any standard algorithms, which forms a great help to secure classified military information or models? The above algorithm is using brute force strategy, meaning it have a tremendous amount of time complexity for a given value of $n = 2$, $k = 3$, and a value of $C = 10$, here we get the number of operations $= C^{(1+3k)}(n+1)^3$, which is operations. This can be further improved by leaving the redundant terms. This algorithm is just based for supercomputers and if it is tested, it will give perfect results, i.e., it will represent all objects in a single equation, further compressing it to a several times depending on how much complex the shape is and hence forming a new way to compress, generate, regenerate and encode objects.

ACKNOWLEDGMENT

I appreciate help received from my father Dr. Jadab Kumar Pal, Deputy Chief Executive, Indian Statistical Institute, Kolkata, for constantly motivating and support to develop this paper. I am thankful to Mr. Bodhiswatta Saha, for constantly inspiring and helping me to design and construct the simulations, which couldn’t have been possible without him. I also appreciate the help received from Christopher Brown, University of Rochester, for allowing me to use their pictures in my research paper for demonstration. The authors also acknowledge the help received from Prof. Shalahb Agarwal, HOD of Computer science department, St. Xavier’s College, for his constant support and motivation.

REFERENCES


Authors Profile

Jimut Bahan Pal is a student of Dept. of Computer Science, St. Xavier’s College (Autonomous), Kolkata-700016. He is fluent in Python programming language, and has invented various scraping programs. He is also a member of various online learning communities like Coursera, Stanford Online, edX etc. Being a Machine Learning enthusiast, he has done various minor projects in Machine Learning area. He has also built various RPG games with Unity-3D, and Unity-2D game engines in association with MOOCs. He is an aspiring and curious researcher.

Dr. Asoke Nath is working as Associate Professor in the Department of Computer Science, St. Xavier’s College (Autonomous), Kolkata. He is engaged in research work in the field of Cryptography and Network Security, Steganography, Green Computing, Big data analytics, Li-Fi Technology, Mathematical modelling of Social Area Networks, MOOCs etc. He has published more than 238 research articles in different Journals and conference proceedings.