Volume I, Issue IV
June 2021

American Journal of **Electronics & Communication**

Society for Makers, Artists, Researchers and Technologists,
USA 6408 Elizabeth Avenue SE, Auburn, Washington 98092.
ONLINE ISSN: 2690-2087

American Journal of
Electronics & Communication

'Society for Makers, Artists, Researchers and Technologists (SMART)' is an American publishing house committed to publish high quality research articles which can bring value and momentum to current research in the domain of Electronics and Communication Technology and allied fields. As a part of this, it has started an international journal titled "American Journal of Electronics & Communication".

"American Journal of Electronics & Communication" (AJEC) is an open access, indexed, multidisciplinary peer reviewed journal that provides a platform for academicians and researchers all over the globe, to publish their research articles related to current trends and developments in Electronics and Communication Technology like microwave, semiconductor devices, VLSI, signal processing, communication, Internet of Things, Machine Learning, Artificial Intelligence etc. The main objective of AJEC is to cultivate innovative ideas among young minds and thus provide a proper guidance to the new frontiers and emerging trends in Electronics & Communication Engineering.

The American Journal of Electronics & Communication makes a maximum effort to publish submitted papers as quickly as possible. Primary reviews would be completed within two months. The authors are then requested to make necessary changes/improvements to their manuscripts within a span of two-three weeks. The whole review process fully respects standard Ethical Guidelines for Peer Reviewers.

American Journal of
Electronics & Communication

Editor in Chief

Managing Editor

American Journal of
Electronics & Communication

Associate Editor

Dr. Samuel Kozaitis

Florida Institute of Technology

Research Interest: Development of algorithms to reduce noise in signals and images, magneto optic and ferroelectric materials, advanced signal processing algorithms ,wavelet-based processing and higher-order correlations.

Dr. Veton Kepuska

Florida Institute of Technology

Research Interest: Neural networks, language modeling, digital signal processing, biometrics, adaptive filtering, telematics, speech recognition, speaker identification, pattern recognition, text to speech.

Dr. Ashiq Adnan Sakib

Florida Polytechnic University

Research Interest: Asynchronous Design, Advanced Digital Design, Low-power Design, and Formal Verification.

Contents

American Journal of Electronics & Communication

Dr. Pravir Malik, American Journal of Electronics & Communication, Vol. I (4), 1-12

A Light-Space-Time Quantum-Computational Model of Subtle-DNA & Genetics

Dr Pravir Malik
Deep Order Technologies, USA
pravir.malik@deepordertechnologies.com

Abstract— Subtle-DNA can be thought of as a conceptual-construct consisting of a double-helix structure, arranged as a light-based downward-strand and a time-based upward-strand. Light imagined existing at different constant speeds far greater than the known speed of c – 186,000 miles per second - offers a unique view of quanta and quantum computation, and the precipitation of such light from higher to lower speeds offer insight into the conceptual downward-strand of subtle-DNA. Such a downward-strand structures an involutionary-reality that seeds space, and subsequently becomes the basis of an evolutionary-reality structured as a time-based upward-strand of subtle-DNA. Analyses of such a composite light-space-time structure further provides a unique point of view into the origin and possibilities of genetics. Genetics can be seen as having a diverse light-based functional, as opposed to a solely form-based foundation. Genetics can also be perceived as being the output of a persistent quantum-level computation. Such a modeling provides useful hypotheses into the subtle conceptual structure of DNA, into the architecture of mutation and the likely processes of constructive and destructive mutation, and the mechanism of heredity. Further the relationship and possible impacts of the quantum-based processes of entanglement and superposition on genetics, and future possibilities due to practically infinite amount of information in antecedent layers of light can be constructed.

Keywords— ***Genetics, Mutation, Quantum Computation, Heredity, Symmetries in Light, Superposition, Entanglement, Genetic-Type Information, Quanta, Upward-Strand, Downward-Strand, Double-Helix***

I. Introduction

The Cosmology of Light computational model (Malik 2018a, b; 2019, 2020) explored a mathematical structure of Light composed of light traveling at different constant speeds beyond the known speed of light, of c – 186,000 miles per second in vacuum - in the physical universe. Light at different speeds engenders different realities, which will be summarized in Sections II and III, and as a result engenders different kinds of information. This vast variety of information is proposed as being the origin of genetic-type information and genetics.

Light at different speeds, from an imagined speed of infinite miles per second, down to c - 186,000 miles per second in vacuum - creates different though mathematically symmetrical realities based on four underlying properties suggested to be implicit in light. This gives rise to a quaternary-based multi-layered mathematical structure in which the unity of light traveling infinitely fast separates in an increasing display of distinct functionality to create the reality of infinite functional diversity we are familiar with in this reality where light travels at c. This happens through a process of precipitation. This process of precipitation can also be perceived as a "subtle" backbone or strand not unlike the backbone or downward-strand of the double-helix DNA structure that animates every living cell.

Such a downward-strand structures an involutionary-reality in which the seeds of functionality are grounded in the matrix of space and form the basis of a time-based evolutionary-action that thereby structures an upward-

strand of subtle-DNA. In other words, the very basis of genetic structure may potentially be tied to the process of precipitation of light, and its subsequent unfolding through time-dynamics.

Further, as light slows down the codification implicit in the state where it is imagined travelling infinitely fast begins to further materialize and generates "libraries" of information as it were, that are accessible to all subsequent layers created by "slower" light. These libraries are the bases of genetic information and heredity.

The process of mutation will be seen to vary depending on which layer of light is involved. Massively significant mutations such as took place on the SRY gene and led to the evolution of human from the chimpanzee species (Ridley, 1999) are suggested to be due to layers of light traveling faster than c. By contrast degenerative mutation leading to dysfunction and disease are hypothesized to be linked to the layer of reality so set up by light projected at slower than c speeds or zero speed.

Section IV will review the action of time-dynamics and suggest a generalized equation for mutational-sequence. Such mutational-sequence is a play of possibilities that have already been seeded in space, due the precipitation action of light forming the downward-strand of subtle-DNA.

Section V integrates the mathematical modeling from the previous sections and arrives at a proposed composite light-space-time quantum-computational model of genetics.

Section VI will review all the afore-mentioned genetic concepts from the point of view of a light-space-time-based quantum-computational model.

Section VII will summarize and conclude with some thoughts on future directions of genetic research in such a light-space-time-based quantum-computation model.

II. Light And The Origin Of Genetics

Practically, the finite speed of light implies that light will take a finite amount of time to travel from one point to another. This is significant even when viewed at the atomic scale. If there is a source of electromagnetic radiation in the nucleus or due to the electrons changing orbits around a nucleus that radiation will be experienced only a finite time later. It can be inferred that this phenomenon is related to quanta. Energy of quanta is specified by (1), where 'E' is energy of quanta, 'h' is Planck's constant, $'\upsilon'$ is frequency of the radiation. Hence (1):

$$E = h\upsilon$$

Eq. 1: Energy of Quanta

Further, the speed of light 'c', frequency of radiation $'\upsilon'$, and wavelength of radiation $'\lambda'$, are related by (2):

$$c = \upsilon\lambda$$

Eq. 2: Speed of Light

Combining (1) and (2) the inverse relationship between c and h can be observed in (3) for any fixed level of 'E':

$$E = \frac{hc}{\lambda}$$

Eq.3: Inverse Relationship Between c and h

Assume now a thought experiment to bring home the creative nature of light and why all of life would possibly emerge from it. Imagine light traveling at an infinite speed. If this were so then the inverse relationship between c and h would necessitate that h approach 0. In other words matter would be unable to form. Conversely if light were to slow down, to approach c, then h would progressively increase to some threshold where energy is able to sustain itself in quanta and matter would emerge. So finite speed of light creates quanta, which creates matter. Therefore all of matter emerges from light.

Note that such an interpretation of quanta suggests that quantum computation needs to be thought of differently than we currently think of it as. This was examined in 'Light-Based Interpretation of Quanta and its Implications on Quantum Computing' (Malik, 2020) and in The Emperor's Quantum Computer (Malik, 2018b). Further, every act of computation yields an output. It is proposed that genetic-type information is the output.

Additionally, in this view it can be seen that the big bang is nothing other than light slowing down and creating matter as a result of that (Malik, 2018a). So if all matter is an action of light then any universe arising is

only a result of it. There are then likely some overarching properties that would be true of light and therefore also true of everything that was to arise in any such universe. It may even be that these properties would be fundamental and would determine structure of matter and everything that emerges out of it.

So, what can be inferred about the properties of light?

The speed of light is known to have implications on the experienced nature of reality. The finiteness, c, at 186,000 miles per second in a vacuum, creates an upper bound to the speed with which any physical object may travel. This also implies that objective reality will be experienced as a past, a present, and a future, from the point of view of that object (Einstein, 1995). These characteristics – a past, a present, and a future – can therefore be thought of as implicit in the nature of light and become part of objective reality because of the speed of light.

Further, it can be observed that c also creates a lower bound when inverted (1/c) being proportional to Planck's constant, h. 'h' as we know pegs the minimum amount of energy or quanta required for expression at the sub-atomic level (Isaacson, 2008). Planck's constant, h, therefore allows matter to form (Lorentz, 1925) and for the reality of nature with a past, present, and future, to also be progressively experienced as a phenomena of connection between seemingly independent islands of matter. This characteristic of 'connection' is therefore also proposed to be implicit in the nature of light and becomes part of objective reality because of the speed of light.

As suggested in The Fractal Organization (Malik, 2015) a 'present' equates to 'vitality' because in the present there is a working out of the play of forces where the most energetic, powerful, or 'vital' force will express itself over others. 'A 'past' equates to 'physicality' because all can be viewed as established reality, as defined by what the eye or other lenses of perception can see. Such lenses see what has already 'physically' been formed in time. A 'future' equates to 'mentality' since cause, or seed, or direction, implies meaning that drives the emergence of phenomena.

These implicit characteristics – physical, vital, mental, connection – of the nature of light as experienced at the layer of reality set up by a finite speed of light may hence be summarized by (4). C_U refers to the speed of light of 186,000 miles per second, that has created the perceived nature of reality, U:

$$C_U: [Physical, Vital, Mental, Connection]$$

Eq. 4: Nature of Light at c

It is known however that at quantum levels the nature of reality is at least characterized by wave-particle duality. Light and matter may be experienced as both particles and waves (Feynman, 1985; De Broglie, 1929; Ekspong 2014). Such duality, as will be explored shortly is related to the notion of quantum. But for matter to be experienced as waves implies that 'h' has become a fraction of itself, $h_{fraction}$. This further implies that c must have become greater than itself, c_N, such that the inequality specified by (5) holds:

$$c_N > c_U$$

Eq. 5: Inequality of Speed of Light

Note that what is implied here is that there must be another nature of reality specified by N that is the result of a speed of light greater than 186,000 miles per second, just as there is a nature of reality specified by U that is the result of the speed of light being 186,000 miles per second. This is consistent with recent developments in physics with the notion of property spaces being separate from but influencing physical space as explored by Nobel Physicist Frank Wilczek (Wilczek, 2016).

It is also to be noted that in Perkowitz's recent treatment of today's breakthroughs in the science of light (Perkowitz, 2011) he suggests that the theory of relativity does not disallow particles already moving at speed c or greater.

It stands to reason that current instrumentation, experience, and normal modes of thinking having developed as a bi-product of the characteristics so created in the layer of reality U may be inadequate to access N without appropriate modification.

The notion of wave-particle duality already challenges the notion of normal thinking perhaps because particle-like phenomena may be viewed as a function of less than or equal to c motion, while wave-like phenomena may be viewed as a function of faster than c motion. That these may be happening simultaneously is reinforced by principles such as complementarity in which experimental observation may allow measurement of one or another but not of both (Whitaker, 2006).

III. Genetic-Type Information In Light

But then taking this trend of a possible increase in the speed of light to its limit, this will result in a speed of light of infinite miles per second. The question is, what is the nature of reality when light is traveling at infinite miles per second? And what kind of information would be created in that reality?

In any space-time continuum be it an area or volume, regardless of scale, light originating at any point will instantaneously have arrived at every other point. Hence light will have a full and immediate *presence* in that space-time continuum. Further, that light will *know* everything that is happening in that space-time instantaneously – that is know what is emerging, what is changing, what is diminishing, what may be connected to what, and so on - or have a quality of *knowledge*. It will connect every object in that space-time completely and therefore have a quality of connection or *harmony*. Finally nothing will be able to resist it or set up a separate reality that excludes it and hence it will have a quality of *power*.

These implicit characteristics of the nature of light as experienced at the layer of reality set up by light traveling infinitely fast may hence be summarized by (6), where c_∞ refers to the speed of light of ∞ miles per second, that has created the perceived nature of reality, ∞:

$$c_\infty : [Presence, Power, Knowledge, Harmony]$$

Eq. 6: Nature of Light at ∞

But it can also be noticed from (4) that 'physical' is related to presence, 'vital' is related to power, 'mental' is related to knowledge, and 'connection' is related to harmony.

The question then, is how do these apparent qualities at ∞ precipitate, translate into, or become the physical-vital-mental-connection based diversity experienced at U? This may be achieved through the intervention or action of a couple of mathematical transformations. First, the essential characteristics of Presence, Power, Knowledge, Harmony that it is posited exist at every point-instant by virtue of the ubiquity of light at ∞ will need to be expressed as sets with up to infinite elements. Such a precipitation is none other than an act of quantization since something implicit in the layer where light travels faster is collecting in 'quanta' to be expressed more materially in the layer where light travels slower. Second, elements in these sets will need to combine together in potentially infinite ways to create a myriad of seeds or signatures that then become the source of the immense diversity experienced at U. This, similarly, is also an act of quantization or the action of a quantization-function. This suggests that all that is seen and experienced at U may be nothing other than 'information' or 'content' of light and as such that there are fundamental mathematical symmetries at play where everything at U is essentially the same thing that exists at ∞.

It may also be inferred that wherever wave-particle duality exists, it does so because of a more observable quantum-translation from one speed of light to another, through the device of quanta.

Assuming that the first transformation occurs at a layer of reality K where the speed of light is c_K, such that $c_U < c_K < c_\infty$, this may be expressed by (7):

$$c_K : [S_{Pr}, S_{Po}, S_K, S_H]$$

Eq. 7: Nature of Light at K

S_{Pr} signifies 'Set of Presence' and may have elements associated with the qualities of being present everywhere, or of creating a physical basis in or on which other functions or characteristics can manifest. Hence S_{Pr} may have elements as expressed by (8):

$$S_{Pr} \ni [Service, Diligence, Perseverance, Stability, \dots]$$

Eq. 8: Set of Presence

S_{Po} signifies 'Set of Power' and may have elements associated with the qualities of being powerful, or of the play of vitality and experimentation which creates all possibility. Hence S_{Po} may have elements as expressed by (9):

$$S_{Po} \ni [Power, Energy, Adventure, Experimentation, \dots]$$

Eq. 9: Set of Power

S_K signifies 'Set of Knowledge' and may have elements associated with the qualities of knowledge, or the search and codification of knowledge. Hence S_K may have elements as expressed by (10):

$$S_K \ni [Knowledge, Making\ of\ Laws, Spread\ of\ Knowl., \dots]$$

Eq. 10: Set of Knowledge

S_H signifies 'Set of Harmony' and may have elements associated with the qualities of harmony, or creating relationship and love. Hence S_H may have elements as expressed by (11):

$$S_H \ni [Harmony, Relationship, Love, Specialization, \dots]$$

Eq. 11: Set of Harmony

Equations (8 - 11) then, shed insight not only into the nature of reality in light's precipitation toward speed c, but also the type of information that may be generated in this precipitation. This information, it is proposed, is genetic-

type information, and has a bearing on information that materializes in genes in the layer of reality where light travels at speed c.

Assuming that the second transformation occurs at a layer of reality N where the speed of light is c_N, such that $c_U < c_N < c_K < c_\infty$, this may be expressed by (12):

$$c_{N:}\, f(S_{Pr}\ x\ S_{Po}\ x\ S_K\ x\ S_H)$$

Eq. 12: Nature of Reality at N

The unique seeds are therefore a function, f, of some unique combination of the elements in the four sets S_{Pr}, S_{Po}, S_K, S_H. This also suggests the basis of vast genetic diversity, due to the functional variety of information available in layers of light antecedent to the layer traveling at c.

The relationship between the layers of light may be hypothesized by the following matrix (13):

$$\begin{bmatrix} c_\infty: [Pr, Po, K, H] \\ (\downarrow\ R_{C_K} = \ f(R_{C_\infty})) \\ c_K: [S_{Pr}, S_{Po}, S_K, S_H] \\ (\downarrow\ R_{C_N} = \ f(R_{C_K})) \\ c_{N:}\, f(S_{Pr}\ x\ S_{Po}\ x\ S_K\ x\ S_H) \\ (\downarrow\ R_{C_U} = \ f(R_{C_N})) \\ c_U: \ [P, V, M, C] \end{bmatrix}_{Light}$$

Eq. 13: Relationship Between Layers of Light

The matrix suggests a series of transformations leading from the ubiquitous nature of light implicit in a point – presence, power, knowledge, harmony - to the seeming diversity of matter observed at the layer of reality U which is fundamentally the same presence, power, knowledge, and harmony projected into another form of itself.

The first transformation is summarized by (14):

$$R_{C_K} = \ f(R_{C_\infty})$$

Eq. 14: First Transformation

This is suggesting that the reality at the layer specified by the speed of light c_K, R_{C_K} is a function of the reality at the layer specified by the speed of light c_∞. This transformation translates the essential nature of a point into the sets described by (8 – 11). Note that (14) is essentially a quantization-function, in that something of the reality of light existing at R_{C_∞}, is translated into reality experienced at R_{C_K}.

The second transformation is summarized by (15):

$$R_{C_N} = \ f(R_{C_K})$$

Eq. 15: Second Transformation

This is suggesting that the reality at the layer specified by the speed of light c_N, R_{C_N} is a function of the reality at the layer specified by the speed of light c_K. This transformation combines elements of the sets into unique seeds as suggested by (12). This transformation can also be thought of as the result of a quantization-function such that something of R_{C_K} is collected as unique seeds at R_{C_N}.

The third transformation is summarized by (16):

$$R_{C_U} = \ f(R_{C_N})$$

Eq. 16: Third Transformation

This is suggesting that the reality at the layer specified by the speed of light c_U, R_{C_U} is a function of the reality at the layer specified by the speed of light c_N. This transformation builds on the unique seeds suggested by (12) to create the diversity of U as specified by (4). This transformation is therefore also the result of a quantization-function such that the seed-aspect of R_{C_N} is translated into the immense diversity experienced at R_{C_U}.

In this framework the notion of wave-particle duality hence may become complementary block-field-wave-particle quadrality where block refers to phenomenon resident to ∞, field to phenomenon resident to N, wave to phenomenon resident to K, and particle to phenomenon resident to U. The essential translation from one level to the next is due to a series of quantization-functions, so that (13) essentially summarizes an algorithm for life (Malik at al., 2019), where an implicit quaternary basis of presence, power, knowledge, and harmony, sets up potentially infinite number of elements derived from sets of presence, power, knowledge, and harmony. The implication of this is that quantization, and in fact this genre of *quantum computation* that arbitrates a structure as summarized by (13) is fundamentally creative, resulting in the vast variety of genetic-type information. As such quantum computation should be thought of as a fundamentally creative process arbitrating abstract possibilities in Light into a rich variety of genetic-type information, that subsequently express itself in material existence.

Equation (13), with modification, can also be expressed as a light-based quantum computational model of genetics as in Eq (17). In this modification it is assumed that light is projected at zero-speed which would effectively create the opposite reality to light existing at infinite speed. Hence in (17) c_0 implies light at zero-

speed, and D, W, I, and C imply Darkness, Weakness, Ignorance, and Chaos, the opposites of Presence, Power, Knowledge, and Harmony, respectively:

$$\begin{bmatrix} c_\infty\colon [Pr, Po, K, H] \\ (\downarrow R_{C_K} = f(R_{C_\infty})) \\ c_K\colon [S_{Pr}, S_{Po}, S_K, S_H] \\ (\downarrow R_{C_N} = f(R_{C_K})) \\ c_N\colon f(S_{Pr}\ x\ S_{Po}\ x\ S_K\ x\ S_H) \\ (\downarrow R_{C_U} = f(R_{C_N})) \\ c_U\colon [P, V, M, C] \\ \Uparrow \\ c_{0\colon [D,W,I,C]} \end{bmatrix}_{Light}$$

Eq. 17: Light-Based Quantum-Computational Model of Genetics

IV. Examination Of A Time-Based Upward Strand Of Subtle-DNA & Generalized Architecture Of Mutational-Sequence

The previous section proposed an essential framework for a light-based quantum-computational model of genetics. This model highlighting a process of precipitation sets up a downward-strand of subtle-DNA, and in this section the compression of such possibility into 'space' is considered to shed insight into an upward-strand of subtle-DNA recognizable through the action of time. Such an upward-strand is organic in nature suggesting likely paths or mutational-sequences determined by what sets of influences are active. Yet the possibilities are wholly determined by the downward-strand and the overarching organizational principles it puts in place in its precipitating scheme from an infinite to zero speed.

Hence, starting with the physical, which recall is suggested as being a projection of Light's property of Presence, an equation, Equation 18, is summarized as:

$$Physical = \begin{bmatrix} M_3 \rightarrow System_{Pr} \\ (\uparrow F \rightarrow I) \\ M_2 \rightarrow S_{System i_{Pr}} \\ (\uparrow Sig \rightarrow F) \\ M_1 \rightarrow Sig_P \\ (\uparrow > P_P) \\ U \rightarrow Physical_U \end{bmatrix} TC \rightarrow Physical_T$$

$$Where \begin{bmatrix} Physical_U \ni [inertia, lethargy, status\ quo, \dots] \\ Physical_T \ni [adaptability, durability, strength, \dots] \end{bmatrix}$$

Eq 18: Possible Mutational-Sequence in Physical-Type Systems

Essentially this equation is laying out the conditions of moving from the untransformed or negative physical state represented by $Physical_U$ to the transformed or positive physical state represented by $Physical_T$.

The first matrix should be read from the bottom to the top:

$$\begin{bmatrix} M_3 \rightarrow System_{Pr} \\ (\uparrow F \rightarrow I) \\ M_2 \rightarrow S_{System_{Pr}} \\ (\uparrow Sig \rightarrow F) \\ M_1 \rightarrow Sig_P \\ (\uparrow > P_P) \\ U \rightarrow Physical_U \end{bmatrix}$$

Hence, at the bottom is the starting point '$U \rightarrow Physical_U$' which identifies the default or untransformed (U) level of the physical. The next row up, $(\uparrow > P_P)$, states that when the patterns of the untransformed physical (P_P) have been overcome (>), movement to the next level ($\uparrow$) is facilitated. Breaking through to the next level, $M_1 \rightarrow Sig_P$, allows its dynamics to become active. Hence, the signature or uniqueness of the physical (Sig_P) becomes active at meta-level 1 (M_1). As this signature becomes more like a Force ($Sig \rightarrow F$), the conditions for breakthrough ($\uparrow$) to the next level are achieved. This next level is referred to as meta-level 2 (M_2), and indicates that the architectural forces represented by the set of system-presence ($S_{System_{Pr}}$) have become more consciously active. When this Force becomes Integral ($F \rightarrow I$) then the conditions for breakthrough ($\uparrow$) to the next level are achieved. The next level is notated as M_3 for meta-level 3, and the dynamics here indicate that the equation for system-presence becomes active. Becoming active basically means that the respective meta-level dynamic begins to act at the once 'untransformed' level (U) further modifying it. Modification or transformation began when M_1 became active. Transformation is accelerated when M_2 becomes active, and even further accelerated when M_3 becomes active.

The rate of the transformation can be better envisioned when considering action of the Transformation Circle, or TC. The TC can be thought of as 4 concentric circles, with M_3 at the center. M_3 is surrounded by M_2, which is

surrounded by M_1. The outer circle is U. If TC is considered to be a clock, than at time 't = 0', the 'physical' can be thought of as being entirely in U. The clock starts ticking only when some initial patterns P_P are overcome ($>P_P$). From this point on as time proceeds the conditions for breakthrough become riper, and a sinusoidal wave begins to integrate more of the concentric circles together. The sinusoid wave (sin) is itself modulated by an euler function, e^x, where 'x' is determined by the strength to overcome patterns (↑) which will likely vary over time but will likely tend to be positive once the clock has started ticking because of the joy experienced with progressive movement. Being that the limit is the outer boundary of the concentric circles, there is further modulation by π until the 4 concentric circles have been integrated. TC, hence, may be represented by Equation 19:

$$TC \equiv (> P_P) \rightarrow \text{mod}\,(\sin, e^x, \pi)$$

Eq 19: Transformation Circle

Hence, the initial nature of the physical that may be characterized by the set comprising of elements such as, lethargy, acceptance of the status quo, amongst other such elements, is represented by:

$$(Physical_U \ni [inertia, lethargy, status\ quo, \dots])$$

This transforms into a physical more characterized by elements such as adaptability, durability, strength, and so on. That is:

$$(Physical_T \ni [adaptability, durability, strength, \dots)$$

This transformation represents the inherent creativity-dynamic driving any mutation sequence within physical-type systems.

Similarly, the equation for the 'Vital', Equation 20, which recall is suggested as being a projection of Light's property of Power, also shows the built-in transformation that represents the innovation-dynamic within the vital:

$$Vital = \begin{bmatrix} M_3 \rightarrow System_P \\ (\uparrow F \rightarrow I) \\ M_2 \rightarrow S_{System_P} \\ (\uparrow Sig \rightarrow F) \\ M_1 \rightarrow Sig_V \\ (\uparrow > P_V) \\ U \rightarrow Vital_U \end{bmatrix} TC \rightarrow Vital_T\,,$$

$$Where \begin{bmatrix} Vital_U \ni [aggression, exploitation, \dots] \\ Vital_T \ni [energy, adventure, enthusiasm, \dots] \end{bmatrix}$$

Eq 20: Possible Mutational-Sequence of Vital-Type Systems

The equation for the 'Mental', Equation 21, which recall is suggested as being a projection of Light's property of Knowledge, is similarly summarized as:

$$Mental = \begin{bmatrix} M_3 \rightarrow System_S \\ (\uparrow F \rightarrow I) \\ M_2 \rightarrow S_{System_S} \\ (\uparrow Sig \rightarrow F) \\ M_1 \rightarrow Sig_M \\ (\uparrow > P_M) \\ U \rightarrow Mental_U \end{bmatrix} TC \rightarrow Mental_T$$

$$Where \begin{bmatrix} Mental_U \ni [fixation, fragmentation, \dots] \\ Mental_T \ni [understanding, imagination, \dots] \end{bmatrix}$$

Eq 21: Possible Mutational-Sequence of Mental-Type Systems

The equation for the 'Integral', Equation 22, suggested as being a projection of Light's property of Harmony, is similarly summarized as:

$$Integral = \begin{bmatrix} M_3 \rightarrow System_N \\ (\uparrow F \rightarrow I) \\ M_2 \rightarrow S_{System_N} \\ (\uparrow Sig \rightarrow F) \\ M_1 \rightarrow Sig_I \\ (\uparrow > P_I) \\ U \rightarrow Integral_U \end{bmatrix} TC \rightarrow Integral_T$$

$$Where \begin{bmatrix} Integral_U \ni [possession, usurpation, hidden\ agendas, \dots] \\ Integral_T \ni [appreciation, shift\ POV, MPV, synthesis, \dots] \end{bmatrix}$$

Eq 22: Possible Mutational-Sequence of Integral-Type Systems

The preceding equations can be generalized by Equation 23:

$$Mutational - Sequence_{orientation-x} = \begin{bmatrix} M_3 \rightarrow System_X \\ (\uparrow F \rightarrow I) \\ M_2 \rightarrow S_{System_X} \\ (\uparrow Sig \rightarrow F) \\ M_1 \rightarrow Sig_x \\ (\uparrow > P_x) \\ U \rightarrow x_U \end{bmatrix} TC \rightarrow x_T\,, where \begin{bmatrix} x_U \ni [\dots] \\ x_T \ni [\dots] \end{bmatrix}$$

Eq 23: Generalized Mutational-Sequence Equation

In this generalized equation, $Mutational - Sequence_{orientation-x}$, refers to the inherent innovation or mutation-possibility within a specific

orientation. Orientation refers to the physical, the vital, the mental, or the integral.

V. Toward A More Complete Light-Space-Time Quantum-Computational Model of Genetics

The previous section provides insight into a generalized equation of mutational sequence. This can be summarized as an evolving-form as in Equation 24:

$$Mutational-Sequence_{orientation-x} = \left(\begin{bmatrix} M_3 \rightarrow System_X \\ (\uparrow F \rightarrow I) \\ M_2 \rightarrow S_{System_X} \\ (\uparrow Sig \rightarrow F) \\ M_1 \rightarrow Sig_x \\ (\uparrow > P_x) \\ U \rightarrow x_U \end{bmatrix} TC \rightarrow x_T \, , where \begin{bmatrix} x_U \ni [\dots] \\ x_T \ni [\dots] \end{bmatrix} \right)_{\langle x_U | x_T \rangle}$$

Eq 24: Evolving Form of Generalized Equation of Mutational-Sequence

The added notation of $\langle x_U | x_T \rangle$ implies that the output of the previous iteration of the equation of innovation, x_T, where the subscript T implies relatively-transformed, now becomes the input, x_U, for the next iteration of the equation, where U implies relatively-untransformed. Hence through time there is greater and greater transformation that pushes experienced reality to greater and greater levels of functional-richness.

But further, given that quanta are proposed to be a doorway to deeper worlds of Light, that in fact allow aspects of those worlds or layers to become active at the surface layer U, the question is when have those aspects become active in manifest time. The following timeline based on generally accepted models of universal history (Particle Data Group, 2015) suggests when. Note too that the subsequent sections of exploring pre-genetic and genetic information at the levels of the electromagnetic spectrum, matter, and life, will explore in far greater detail some of the statements made in the following timeline:

- At time, $t \leq 0$ seconds, only M_3 is active, and then remains active for all $t < \infty$. Recall that M_3 represents the four-fold reality present in every ubiquitous-point-instant.
- At time, $0 \geq t > \infty$, M_2 the set of architectural forces continually gets added to, thereby increasing the size of the sets of forces.
- At time, $t \geq 0$, space, time, energy, gravity, the first clear expression of the four-fold order, emerges. This first expression is significant because it sets in motion the interplay between the antecedent quantum-layer and the layer where matter will materialize. Note that the antecedent quantum-layer likely houses the ever-enhanced four-base logic-encoding ecosystems critical to genetics and evolution.
- At time, $0 > t \geq 10^{-36}$ seconds, the equation of Innovation, $Innovation_{orientation-x}$, is such that M_1also becomes active. The activation of M_1 begins to result in unique expressions or signatures of the set of architectural forces, and in this case in the reality of the essentially ubiquitous electromagnetic-spectrum (EM Spectrum) as a vehicle of the four-fold order that expressed itself in all that existed and in all that unfolded from that point in time on.
- At time, $t \sim 10^{-10}$ seconds, fundamental particles emerge as an essential material basis of the four architectural forces that frame all further development. As in the case of the EM Spectrum this implies the activity of M_1, and then also of U.
- At time, $t \sim 3 \times 10^5$ years light atoms emerge, and at time $t \sim 10^9$ years heavier atoms in the stars emerge. These also imply the continued activity of M_1 and U.
- At time, $t \sim 13.8 \times 10^9$ years, a further clear expression of the same fourfold order as the bases of an even more complex organization, that of cellular life and all that is founded on it comes into being. This time-point will be represented by the notation $t \sim E_{Cell}$, where 'E' stands for emergence. This too implies the activity of M_1. Note that the sets of architectural forces specified by M_2 continue to increase the number of elements they comprise of as the complex interaction between the layers continues.
- At time $t > 13.8 \times 10^9$ years, human-beings, and more complex social organizations emerge. Here TC acts with an implicit direction of operation from U to M_3. This time-point will be represented by $t \sim E_{Human}$.
-

Note that the emergence of space-time-energy-gravity, and subsequently of the electromagnetic spectrum, quantum particles, and atoms, implies that any possible pre-genetic information in their conceived four-base logic-encoding ecosystems

must also be present in some form in genes as appear later with the advent of cellular life. As such, the logic of cosmic fundamentals and of the very basis of matter is deeply ingrained in all things, inanimate and animate.

Based on the aforementioned timeline and description Equation 25 for Emergence true of any space-time scale may be generalized as the following:

$$Emergence_{space-time} = \left| \begin{matrix} \begin{bmatrix} M_3 \rightarrow System_X \\ (\uparrow F \rightarrow I) \\ M_2 \rightarrow S_{System_X} \\ (\uparrow Sig \rightarrow F) \\ M_1 \rightarrow Sig_x \\ (\uparrow > P_{x)} \\ U \rightarrow x_U \end{bmatrix}_{Space} \\ \begin{bmatrix} M_3 : -\infty \leq t \leq \infty \\ \downarrow \\ M_2 : 0 \geq \mathrm{t} > \infty \\ \downarrow \\ M_1 : 0 > \mathrm{t} > \infty \\ \downarrow \\ U \rightarrow \begin{matrix} \mathrm{t} \leq E_{Cell}; \mathrm{TC}: M_3 \rightarrow \mathrm{U} \\ \mathrm{t} \sim E_{Human}; \mathrm{TC}: U \rightarrow M_3 \end{matrix} \end{bmatrix}_{Time} \\ TC \rightarrow x_T \text{ , where } \begin{bmatrix} x_U \ni [\dots] \\ x_T \ni [\dots] \end{bmatrix} \end{matrix} \right|_{\langle x_U | x_T \rangle}$$

Eq 25: Space-Time Emergence

An implication of this equation, brought out more explicitly through the elaboration of the 'Time' component, is that the layers U, M_1, M_2, and M_3 exist simultaneously. Adding the 'Light-Matrix' derived in Sectoin III enhances Equation 25 to the Light-Space-Time Emergence form as represented by Equation 26:

$$Emergence_{light-space-time} = \left| \begin{matrix} \begin{bmatrix} c_\infty : [Pr, Po, K, H] \\ (\downarrow R_{C_K} = f(R_{C_\infty})) \\ c_K : [S_{Pr}, S_{Po}, S_K, S_H] \\ (\downarrow R_{C_N} = f(R_{C_K})) \\ c_N : f(S_{Pr}\ x\ S_{Po}\ x\ S_K\ x\ S_H) \\ (\downarrow R_{C_U} = f(R_{C_N})) \\ c_U : [P, V, M, C] \\ \Uparrow \\ c_{0:[D,W,I,C]} \end{bmatrix}_{Light} \begin{bmatrix} M_3 \rightarrow System_X \\ (\uparrow F \rightarrow I) \\ M_2 \rightarrow S_{System_X} \\ (\uparrow Sig \rightarrow F) \\ M_1 \rightarrow Sig_x \\ (\uparrow > P_x) \\ U \rightarrow x_U \end{bmatrix}_{Space} \\ \begin{bmatrix} M_3 : -\infty \leq t \leq \infty \\ \downarrow \\ M_2 : 0 \geq \mathrm{t} > \infty \\ \downarrow \\ M_1 : 0 > \mathrm{t} > \infty \\ \downarrow \\ U \rightarrow \begin{matrix} \mathrm{t} \leq E_{Cell}; \mathrm{TC}: M_3 \rightarrow \mathrm{U} \\ \mathrm{t} \sim E_{Human}; \mathrm{TC}: U \rightarrow M_3 \end{matrix} \end{bmatrix}_{Time} TC \rightarrow x_T \end{matrix} \right|_{\langle x_U | x_T \rangle}$$

Eq 26: Light-Space-Time Emergence

In (26) there is a 1:1 mapping between the Light and Space matrices in that M_3 reflects the ever-present C_∞, M_2 reflects C_K, M_1 reflects C_N, and U reflects C_U. The Time matrix simply gives estimates at which time each of the layers became active.

VI. Key Concepts of Genetics From the Light-Based Point Of View

1) The Origins of Genetics

The infinite information codified in Light is the origin of genetics. As discussed previously Light in its state where it travels infinitely fast, possesses characteristics of presence, power, knowledge, and harmony, and contains vast possibility within it. This vast possibility can be thought of as information, and its structure related to the four characteristics, as the basis of genetics.

2) The Light-Based Downward-Strand

All-possibility that exists in the reality of light traveling infinitely fast is progressively materialized through a mathematical arrangement by which the subtle-infinite becomes the astounding material-diversity experienced when light travels at c. The mathematical process, by which this transformation takes place, creates the light-based downward-strand.

3) The Time-Based Upward-Strand

The possibilities seeded in the structure of space arise or mature through the passage of time, and this process is summarized by the Space-Matrix or upward-strand.

The fundamental structure of the upward-strand mirrors the downward-strand and its possibilities are intimately tied to the levels that exist in the downward-strand.

4) The Essential Structure of Subtle-DNA

The essential structure of subtle-DNA comprises of a largely pre-existent Light-Matrix or downward-strand and a resulting Space-Matrix or upward-strand. Libraries of subtle pre-genetic information exist in the downward-strand. Genetic-type information expresses itself through the upward-strand as it were, and is due to the interaction between the possibilities embodied by the downward and upward strands.

5) Subtle-Libraries of Pre-Genetic Information

The progressive materialization of light has been modeled by a series of mathematical transformations in the Sections II and III. These transformations take the vast amount of information existing where light travels infinitely fast, to effectively create a series of precipitated subtle-libraries also of practically infinite pre-genetic information. This series of subtle-libraries subsequently allows infinite material diversity to come into being.

6) Material-Fabric

Just as genetic information is housed in DNA in living cells, there has to exist some structure to house the proposed pre-genetic information that exists at a pre-cellular stage. It is proposed that such pre-genetic information is housed in a structure termed 'Material-Fabric'. This material-fabric exists at the interface or could be the interface between the antecedent quantum-layer and the reality that emerges at c_U.

7) Four-Base Logic-Encoding Ecosystems

Four-base logic-encoding ecosystems are imagined containing logic in the quantum-layer antecedent to the reality emerging at c_U. These four-base logic-encoding ecosystems can be subject to change in the interplay with the material layer and may be related to the processes of mutation.

8) Superposition in Genetics

In the process of quantum-computation, by which four-base logic-encoding ecosystems, the pre-genetic and the genetic libraries, can be altered, the different dynamics representative of realities created by light traveling at different speeds are always present. This presence exists in superposed fashion and the real-time quantum-computation determines which superposed possibility will manifest materially.

9) Entanglement in Genetics

The information inherent to a particular layer, created through light traveling at a different speed, generates libraries of possibility through a mathematical process. Due to different dynamics of space and time representative of the layer created by light at a particular speed, these libraries exist differently in an entangled state, therefore being subtly present or influencing layers of light traveling at a slower speed relative to that layer. Common DNA existing in every cell at the material layer may be thought of as a logical outcome of this process of antecedent-entanglement.

10) Heredity

The presiding or generally accessible four-base logic-encoding ecosystems may be thought of as the primary bases of heredity.

11) Constructive-Mutation

Constructive-mutation is imagined occurring when patterns of a largely obstinate nature at the material level are broken as a result of which other possibilities existing in the higher levels of the light-based downward-strand are allowed to manifest. Of necessity this means that an inherent process of integration is taking place since light is unifying with its deeper nature. Constructive-mutation is intimately tied to this notion of integration.

12) Destructive-Mutation

When obstinate or disintegrating patterns persist or are chosen destructive-mutation will result. In its essence this suggests that light is moving away from its essential unified reality more towards the reality typified by disaggregation, that can be imagined to exists were light to be projected at zero-speed as suggested by c_0 in Eq (17).

13) Interpretation of Matter

Matter is the result of a constant computation involving the existing material layer, the material-fabric, four-base logic-encoding ecosystems, and the antecedent light layers. This means that matter can and will change as the interplay between these layers changes.

14) Evolution and the Possibilities of Genetics

Evolution is a process by which pre-genetic possibilities in antecedent layers of light materialize due to the existence of the right material conditions. This will also imply that the pre-genetic material existing in the four-base logic-encoding ecosystems will change.

15) Post-Genetic Code

In its possibilities of materialization information in light may house itself in subtle-libraries generated at various layers of light, four-base logic-encoding ecosystems at the quantum-level, the material-fabric, or in genetic code in living cells. But it is also possible through the process of evolution that the "structure" housing further possibilities in light may take on a hybrid form that may be referred to as Post-Genetic Code.

VII. Summary and Further Research

The light-space-time quantum-computational model of genetics described in this paper suggests several avenues of further research.

In this model there are multiple layers of light that house different kinds of fourfold information. The model is subject to a persistent quantum computation which creates genetic-type information as its output. In this model the origin of genetics is seen as being the antecedent layers of light traveling faster than c. Such layers of light can mathematically be structured as non-physical property-spaces that impact physical reality. The question is whether such a configuration of light-based property-spaces are valid in terms of thinking about genetics, and further what other kinds of property-space models may be valid as a basis of comparison?

The precipitation of light is suggested to have a bearing on the downward-strand of DNA. This downward-strand forms an involutionary-reality, is seeded as functional possibility or seeds in space, and becomes apparent through the unfolding of time.

Subtle-libraries of genetic-type information are suggested to be inputs in a process of quantum computation that also have a bearing on how genetic information materializes.

In terms of further research, is there indeed such a precipitation in the existing conception of the downward-strand of regular DNA? Is there a corresponding time-based upward-strand seeded in space? Further, is there some relationship between the four nitrogenous bases in DNA of guanine, adenine, cytosine and thymine and the four properties envisioned to be implicit in light?

For such a computational model to be viable there needs to be another housing structure for genetic-type information. It is proposed that there is some kind of 'material-fabric' at the quantum level where light precipitates to light at speed c. Is this indeed the case?

Further, as a result of being at the quantum-level, phenomenon such as superposition and entanglement may also influence genetic information. Is the model of superposition and entanglement proposed briefly in this paper a possible way in which these quantum phenomenon affect genetics?

Persistence of information in such a material-fabric is the basis of heredity. Constructive mutation is due to interaction with layers of light traveling faster than c where the root of all function is proposed to exist. Destructive mutation may be perceived as being due to interaction with light existing at zero-speed, where disaggregation increases. These views of heredity and mutation need to be elaborated further.

If light is indeed the origin of genetics and if light-based processes such have been briefly discussed in this paper are valid, then what are implications for non-invasively and positively influencing processes of genetics? Experiments to begin to check the validity of this possibility can be created.

References

1. De Broglie, L. 1929. The Wave Nature of the Electron. Nobel Lecture.
2. Einstein, A. 1995. Relativity: The Special and General Theory. New York: Broadway Books.
3. Ekspong. 2014. "The Dual Nature of Light as Reflected in the Nobel Archives". *Nobelprize.org*. Nobel Media AB 2014. Web. 15 Oct 2016.

4. Feynman, RP. 1985. QED The Strange Theory of Light and Matter. New Jersey: Princeton University Press
5. Holland, P. 1995. The Quantum Theory of Motion: An Account of the de Broglie-Bohm Causal Interpretation of Quantum Mechanics. Cambridge: Cambridge University Press.
6. Isaacson, W. 2008. Einstein: His Life and Universe. Simon and Schuster. New York.
7. Lloyd, S. 2007. Programming the Universe: A Quantum Computer Scientist Takes On the Cosmos. New York: Vintage
8. Lorentz, H.A. 1925. The Science of Nature. Vol. 25, p 1008. Springer
9. Malik, P. 2015. The Fractal Organization. New Delhi: Sage Publications
10. Malik,P., Pretorius, L., Winzker, D. 2017. Qualified Determinism in Emergent-Technology Complex Adaptive Systems. Conference Proceedings IEEE TEMSON 2017.
11. Malik, P. 2018a. Cosmology of Light. Google Books
12. Malik, P. 2018b. The Emperor's Quantum Computer. Google Books.
13. Malik, P. 2019. The Origin and Possibilities of Genetics. Google Books.
14. Malik, P. Pretorius, L. 2019. An Algorithm for the Emergence of Life Based on a Multi-Layered Symmetry-Based Model of Light. 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). 10.1109/CCWC.2019.8666554
15. Malik, P. "Light-Based Interpretation of Quanta and its Implications on Quantum Computing," 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2020, pp. 0719-0726, doi: 10.1109/CCWC47524.2020.9031279.
16. Particle Data Group. 2015. Lawrence Berkeley National Laboratory. http://www.cpepphysics.org/main_universe/universe.html
17. Perkowitz, S. 2011. Slow Light. London: Imperial College Press
18. Ridley, M. Genome: The Autobiography of a Species in 23 Chapters.. Great Britain: Fourth Estate.
19. Whitaker, A. 2006. Einstein, Bohr and the Quantum Dilemma: From Quantum Theory to Quantum Information. Cambridge: Cambridge University Press
20. Wilczek, F. 2016. A Beautiful Question: Finding Nature's Deep Design. New York: Penguin Books

American Journal of Electronics & Communication

Abhishek Tripathi et. al., American Journal of Electronics & Communication, Vol. I (4), 13-15

A new Modified method of Cryptography using Caesar Cipher

Abhishek Tripathi
Department of Computer Science
University of Engineering and Management
Kolkata, India
abhishek161199@gmail.com

Jhilam Chakraborty
Department of Computer Science
University of Engineering and Management
Kolkata, India
jhilamchakraborty.2001@gmail.com

Sadia Anzum
Department of Computer Science
University of Engineering and Management
Kolkata, India
anzum.sadia@gmail.com

Sudipta Basu Pal
Department of Computer Science
University of Engineering and Management
Kolkata, India
Sudipta_basu68@yahoo.com

Abstract

Nowadays the modern world depends on connections through the internet brings different teams together. The essential components of communication are sender, medium, and receiver. Data transmission over the internet is not possible without any encryption method due to security issues. Different types of areas like corporate sectors, banking sectors, government sectors, and many other sectors share their data through the internet. Hackers always try to attack the transmitted data and try to recover the data. Various techniques are developed for providing data security. Cryptography is used for the safe transmission of data. Encryption is done at the sender side in cryptography, and decryption is done at the receiver side. In the encryption technique, Caesar cipher is one of the best examples. The analysis of Basic Caesar cipher, Delta formation Caesar cipher, and XOR Caesar cipher is done based on many parameters like Avalanche Effect, Frequency Test, and Brute force attack. The authors of this paper have tried to modify the caesar cipher method, which produces ciphertext that can be read. After that with the new ciphertext that can be read, then cryptanalysis not suspicious of the ciphertext.

Keywords

Substitution, Plaintext, Cryptography, Caesar Cipher, Ciphertext

I. Introduction

The meaning of cryptography is simply hiding of data or information. Hiding mainly provides the security from the attackers [1,2,3].In the case of encryption the Caesar Cipher is one of the simplest and earliest methods of cryptography which was first used by the Roman Emperor Julius Caesar to send secret messages to his army generals[4,5,6]. It is a simple replacement cipher where the plaintext is shifted for a pre-defined number of times. This pre-defined number becomes our key. For instance, with a shift of 1, A would be replaced by B, B would be replaced by C, and so on. The main disadvantage of this cipher is the limited number of keys available. With each language coming with a finite set of letters of the alphabet, the resolution also becomes finite for this reason. So with the English language, there are only 26 keys possible. This way a code breaker will try out each possible key and get the exact plaintext.

In this paper authors have applied a modified approach, instead of conventionally shifting the characters linearly, the characters will be shifted arbitrarily[7,8,9,10]. For this case, the substitution permutation box method will be used. A substitution box would be generated by performing the process of Affine Ciphers [Cipher text = (key1*Plain text)+ key2]. Then the characters would be substituted by their corresponding equivalent values. Also, the Ciphertext is scrambled by alternating the position of the characters randomly to conceal the features of the language. This operation is done using double columnar transposition on the plaintext to be encrypted. This algorithm can encrypt the special characters which the conventional Caesar cipher cannot encrypt.

II. Background Work

Roman dictator Julius Caesar was known to use a method of encryption (currently known as *Caesar Cipher)* to convey confidential messages to his army generals.

In the nineteenth century, it was noticed that the advertisement section in newspapers were used to exchange the encrypted message using this method. Caesar cipher was still in use even as late as 1915. It was also used as a replacement of more complex ciphers that were too difficult to decode.

A. ROT-13:

ROT-13 is a kind of Caesar Cipher that was developed in ancient Rome wherein the shift implemented to encrypt is equal to 13. This cipher, however, does not offer any safety

and hence, can be decoded very easily using the hill-climbing technique.

B. Some Modifications:

Some methods have been proposed by the researchers to improve the security level of the traditional Caesar cipher.
The general monoalphabetic method of encryption is mentioned in the book "A Manuscript of Deciphering Cryptographic Messages" written by scientist Abu Alkindi.
In 2013, Dr. A Padmapriya and Dr. P. Subhasri proposed the method of reverse Caesar cipher encryption using all the 256 ASCII characters.

C. Caesar Cipher and Brute-Force Attack

The Brute force attack is a cryptanalytic method where the cryptanalysis makes a guess of the key and decrypts the ciphertext and if the key is incorrect he simply shifts to the next key in consideration [11,12,13,14]. This method is gone by trial and error.
In 2013 a new method was considered that used a two-level transposition which would employ two-level encryption and decryption. Here the Brute force attack is not conceivable because two different key levels have been used during the process of encryption.

III. Result Analysis

A. Implementation of the modified approach

1) The user enters the password and plaintext in the input.
Plaintext: We will be attacked today
Password: advert

2) The two subkeys will be created key A and Hkey B. At the start the Hkey A is set to 0, and password "advert" is converted into its ASCII equivalent.

3) The Hkey A is updated using the following formula,and this step is continued for all values until the final Hkey A obtained is 1367456.

4) We will takethe mod 5 of ASCII equivalent and add1 to it gives Hkey B:
Hence, Hkey A becomes equal to 1367456 and Hkey B becomes equal to 18465.

5) For the next satep, two substitution tables are created by calling initialize function(). 'Table' and 'inverse table' are the names given to them.

6) Substituting the characters of of plain texrt by the assigned values of the 'table' table the ciphertexts generated.
Plaintext: We will be attacked today
Ciphertext: Q^GBaCzzCNY{Yw\fAXy.

B. Result analysis

For performing cryptanalysis on this caesar cipher algorithm, a message with encryption key 'advert' is taken This algorithm is used for the encryption process and the resultant ciphertext is shown as the output. The decryption can be achieved by using the same encryption key. Now, we are assuming that if someone gets this encrypted text but doesn't know the encryption key. Hence, to decrypt the message he uses many cryptanalysis methods.He uses frequency analysis to decode and decrypt the text. Already we have done frequency analysis with 200 different samples on the text which is encrypted therefore the frequency analysis gives incorrect answers protecting out encrypted text. The characteristics of the English language also have been successfully hidden (like the two or three letter words frequently occurring together, like-is, an, he, she, the, etc.) by using the transposition method, making the level of security, even more, stronger for an the person to take advantage of language characteristics to decipher, as well as the range of each character in the key is increased to 255, therefore it is almost impossible to decipher the text using the brute force attack as instead of only 26 possible key combinations, the possible number of combinations of keys is increased to (key length) ^256.

The comparation with the conventional Caesar Cipher with the modified approach of the same technique is shown in table 1. The following table shows the comparison result between the two methods clearly.

TABLE I. Comparison between Classical Caesar Cipher and the Modified Caesar Cipher when used to encrypt and decrypt a text in English.

Classical Caesar Cipher	**Modified Caesar Cipher**
All the characters are shifted linearly by a constant key.	Each character is shifted by a random number using affine cipher.
The characteristics of the language is respected and maintained.	Characters are spread throughout the cipher text. So the characteristics of the language remains hidden
Easy to implement.	It is more complex hence is comparatively difficult to execute.
Prone to attacks like the frequency analysis attacks.	Impossible to attack using the frequency analysis attack method.
Takes only 26 key combinations, hence it is easy to break using the Bruce Force attack.	It takes (key length) ^256 as the possible key combinations. Hence it becomes difficult to break using Brute Force attack.

IV. CONCLUSION

In this paper, the authors have tried to modify the basic caesar cipher method that produces ciphertext that can be read. The advantage of the new method is with the ciphertext can be read, then cryptanalysis is not considered as suspicious of the ciphertext. This algorithm uses a random approach for the substitution of characters present in the sample text. By performing the methods of cryptanalysis on the new algorithm, it was seen impossible to break it by the methods in question (Frequency analysis and the Brute Force technique). Security provided by this modified algorithm of Caesar Cipher can be further enhanced by using it with one or more different encryption algorithms or by using asymmetric key tactics instead of the symmetric key ones.

ACKNOWLEDGMENT

The authors wish to thank all the professors of the Computer Science Engineering Department UEM, Kolkata, India, for a numbers of fruitful discussions and valuable suggestion to perform the analysis.

REFERENCES

[1] S G Srikantaswamy, Dr. H D Phaneendra, "Improved Caesar Cipher with Random Number Generation Technique and Multistage Encryption", International Journal on Cryptography and Information Security (IJCIS). Vol. 2, No.4. pp. 39-49, December 2012.

[2] L .c han, n.m. mahyuddin , ”an implementation of caesar Cipher and xor encryption technique in a secure wireless Communication”,ieee confer,encepp.111-116, 2014.

[3] Goyal,Khasis. Kinger, Supriya.Modified Caesar Cipherfor Better Security Enhancement. International Journal of Computer Aplications (975-8887) Volume 73 - No.3 July 2013.

[4] Practical Cryptography Niels Ferguson and Bruce Schneier, John Wiley & Sons, 2003

[5] Applied Cryptography, 2nd edition Bruce Schneier, John Wiley & Sons, 1996

[6] The Code Book - The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography Simon Singh, Doubleday, 1999

[7] Atul Kahate (2009), Cryptography and Network Security, 2nd edition,

[8] McGraw-Hill. http://searchsecurity.techtarget.com/definition/cipher

[9] Stallings, W. (2006), Cryptography and Network Security 4/E., Pearson Education India.

[10] Behrouz A Fourouzan, Debdeep Mukhopadhyay (2010), Cryptography and Network, 2nd edition, McGraw-Hill.

[11] Goyal, Kashish, and SupriyaKinger. "Modified Caesar Cipher for Better Security Enhancement." International Journal of Computer Applications (0975–8887) Volume (2013).

[12] Singh, Ajit, Aarti Nandal, and Swati Malik. "Implementation of Caesar Cipher with Rail Fence for Enhancing Data Security." International Journal of Advanced Research in Computer Science and Software Engineering 2.12 (2012).

[13] Omolara, O. E., A. I. Oludare, and S. E. Abdulahi. "Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication." Computer Engineering and Intelligent Systems 5.5 (2014): 34-46.

[14] Senthil, K., K. Prasanthi, and R. Rajaram. "A modern avatar of Julius Caesar and Vigenere cipher." Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on. IEEE, 2013.

[15] Disina, Abdulkadir Hassan. "Robust Caesar Cipher against frequency cryptanalysis using bi-directional shifting." Diss. Universiti Tun Hussein Onn Malaysia, 2014.

[16] Purnama, Benni, and AH Hetty Rohayani. "A New Modified Caesar Cipher Cryptography Method with Legible Ciphertext from a Message to be Encrypted." Procedia Computer Science 59 (2015): 195-204.

American Journal of Electronics & Communication

Shuvendu Das et. al., American Journal of Electronics & Communication, Vol. I (4), 16-21

Disease Prediction from Drug Information using Machine Learning

Shuvendu Das[1], Sainik Kumar Mahata[2], Abhishek Das[3], Koushik Deb[4]

[1, 2, 4]Institute of Engineering and Management, Kolkata, India

[3]Bengal College of Engineering, Durgapur, India

[1]getshuvendu97@gmail.com, [2]sainik.mahata@gmail.com

[3]abhishek93.das93@gmail.com, [4]koushik.deb@iemcal.com

Abstract

Drug reviews play a very important role in providing crucial medical care information for both healthcare professionals and consumers. Also, in the absence of an actual practicing healthcare professional, a consumer can look for an online review of drugs before making a purchase. But these reviews are generally unstructured in nature and often do not provide concise information on the disease/nature of the disease, the drugs are prescribed for. In this scenario, a learning model that can be trained to predict the disease/type of disease, when provided with a drug name and its corresponding review, becomes very important. To mitigate the above-mentioned issue, we present and compare various machine learning-based prediction models. Also, the performance of each of the models has been quantified using metrics such as precision, recall, F1-Score, and accuracy.

Keywords

Machine Learning, Deep Learning, Classification, Prediction, Drug Review

1. Introduction

Due to this pandemic situation, where the majority of the population has been confined to their homes and online procurement of goods for daily use is the new normal, reviews of such goods on the online space plays a huge role and acts as a metric by which users can select products without physically feeling and checking them. Moreover, in the case of online shopping for medicines, reviews become even more important as mining on less descriptive, unverified and bogus reviews may become lethal.

Also, due to the absence of certified medical practitioners, most of the users are relying heavily on self-medication. In such a scenario, it becomes very difficult for non-expert users to study reviews of a drug and identify the disease for which the drug is prescribed for. This situation arises as the medicine literature is extremely vast, it becomes very difficult for non-expert users to pin-point on the right medicine, after observing reviews and feedback for the same in the online forums.

Moreover, the reviews and feedback of drugs on online forums are unstructured, which may lead to non-uniform judgement and inability to classify the comments into meaningful insights.

To alleviate the above issues, we plan to develop machine learning models, which when trained using pre-processed and structured medicine reviews, will be able to uniformly predict the name of the disease, for which its usage is intended for. This will serve the objective of enabling users to safely intake the predicted drug with utmost benefit. This will also ensure that users are not bogged down by unexpected side-effects as a result of wrong ingestion.

For developing the learning models, we have used two approaches; one model uses the traditional machine learning algorithms and the second one uses the more recent state-of-the-art deep learning algorithms. When validated, both our models returned high efficiency for metrics such as precision, recall, accuracy and F1 score.

The rest of the paper is organized as follows. Section 2 mentions some of the related work done on this domain in recent years. Section 3 talks about the data source that we used to develop our models and the process of cleaning the data. Section 4 describes the methodology followed for developing the model and also discusses the results of the models. The paper ends with the concluding remarks in Section 5.

2. Related Work

Hu et. al. [1], designed an unsupervised anomaly detection system using a drug review dataset, where they used probability density estimation models to describe the distribution of the data over a number of key attributes and use the model to identify anomalies as points with low estimated probability. The results are validated against cases identified by healthcare domain experts. There was strong agreement between cases identified by the models and expert clinical assessment.

Gräßer et. al. [2], in their work performed multiple tasks over drug reviews with data obtained by crawling online pharmaceutical review sites. They performed sentiment analysis to predict the sentiments concerning overall satisfaction, side effects and effectiveness of user reviews on specific drugs. To meet the challenge of lacking annotated data they further investigated the transferability of trained classification models among domains, i.e., conditions, and data sources. With this work they showed that transfer learning approaches can be used to exploit similarities across domains and is a promising approach for cross-domain sentiment analysis.

Dinh et. al. [3], developed a data-mining model to evaluate the effectiveness and detect potential side effects from online customer reviews on specific prescription drugs. The study utilizes text parsing, text filtering, text topic, and text clustering within SAS Enterprise Miner for feature engineering and supervised learning algorithm for building multiple predictive models (logistic regression, decision tree, neural network, text rule builder) to identify the optimal model for reviews classification. The study's results show that the best predictive model for side effect classification is the text rule builder model with a validation average square error of 5.79% and a misclassification rate of 31.57%. Regarding effectiveness classification, the text rule builder model also works best with 5.10% validation average square error and 29.08% misclassification rate.

Yadav et. al. [4], we present a benchmark setup for analyzing the sentiment with respect to users' medical condition considering the information, available in social media in particular. To this end, we have crawled the medical forum website 'patient.info' with opinions about medical conditions self-narrated by the users. We constrained ourselves to some of the popular domains such as depression, anxiety, asthma, and allergy. The focus is given on the identification of multiple forms of medical sentiments which can be inferred from users' medical condition, treatment, and medication. Thereafter, a deep Convolutional Neural Network (CNN) based medical sentiment analysis system is developed for the purpose of evaluation. The resources are made available to the community through the LRE map for further research.

While most of the recent works on drug reviews focus on sentiment analysis, evaluating side effects and effectiveness of drugs and predicting names of drugs, this is the first work on predicting the disease name from drug reviews that will help users select the optimal drug based on the ailment that they are suffering from.

3. Dataset

For developing our machine learning models, we used the UCI ML Drug Review dataset[1] that had 2,15,063 number of reviews along with drug name and the disease name. Since the data was unstructured and had multiple rogue textual spans, we first needed to pre-process the data to make it suitable for training purposes. These steps included the removal of extra characters to clean the data. The extra characters that

[1] https://archive.ics.uci.edu/ml/datasets/Drug+Review+Dataset+%28Drugs.com%29

were removed/cleaned included mentions, punctuations and URLs. Also, words from hashtags were extracted and extra spaces were contracted.

After cleaning, 53, 498 structured reviews, along with drug name and disease names were extracted. Out of these, 52, 498 such instances were selected as training data and 1,000 instances were selected as test data. As far as the labels were concerned, there were 648 unique labels that were to be predicted.

4. Methodology and Results

For developing the multi-label, machine learning classification models, we used two approaches. The first approach incorporated the traditional machine learning models such as Random Forest and Naïve Bayes algorithms. The second approach incorporated the more state-of-the-art sequential Neural Network algorithm, embodying Long-Short term memory [5] (LSTM) cells. Description of both these approaches are provided in the following subsections.

4.1 Machine Learning model

Since the training data consisted of the drug name and the reviews of the same drug that needed to be mapped to the disease name that was kept as the label, we first decided to concatenate both the drug name and the review. After concatenation, the extended input took the following structure, where the review followed the drug name and an "equal to" sign.

> "Mobic = Reduced my pain by 80% and lets me live a normal life again!"

Also, the labels were passed through a Label Encoder, which encodes target labels with a value between 0 and n_classes - 1, where n_classes in our case was 648.

Thereafter, TF-IDF Vectorizer[2] from the python package sklearn[3], which converts a collection of raw documents to a matrix of TF-IDF features, was used to vectorize the extended input.

Subsequently, the Random Forest algorithm, which is an ensemble learning model, where we can create many decision trees and predict based on the highest voting, was used to build the classification model. We took 100 estimators or trees and 1000 depths to make predictions. This model garnered an accuracy figure of 0.83 when

[2] https://scikit-learn.org/stable/modules/generated/sklearn.feature_extraction.text.TfidfVectorizer.html
[3] https://scikit-learn.org/stable/

tested using the test data. Similarly, F1 score reached 0.75 and precision, recall stopped at 0.89 and 0.72.

Also, the Multinomial Naïve Bayes algorithm was also used to build the same classification model. This model garnered an accuracy score of 0.75 when tested using the test data. Also, F1 score reached to 0.58 and precision and recall stood at 0.82 and 0.59 respectively.

It was noticed that scores of the Random Forest algorithm were better than Naïve Bayes algorithm.

4.2 Deep Learning model

For developing the deep learning model, we used a sequential feed-forward network built using LSTM cells. In this case, the input features, drug names and the reviews, were kept separate and not concatenated, as in the previous experiment. Also, the reviews were passed to through the pre-trained Google News Word Embedding[4] of size 300. This, in turn, produced word vectors of size 300 for the reviews.

Also, a straight-forward model, where no pre-trained embedding was used, was alsodeveloped.

The name of the drug was first passed through an embedding layer. The output of this layer was then concatenated to the word vector of the reviews (both Google News embedding and default embedding) and were passed through two LSTM layers. The output of the LSTM layer was then passed to a dense layer, which mapped the context vector to the respective labels.

The model, with the pre-trained embedding garnered F1 score of 0.80 and scores of 0.82 and 0.79 for precision and recall respectively, when tested using the test data.

Similarly, the model with the default embedding, garnered F1 score of 0.79, and precision and recall scores of 0.83 and 0.77 respectively, when tested using the testdata.

A comparative analysis of the classification scores is shown in Table 1.

[4] https://github.com/mmihaltz/word2vec-GoogleNews-vectors

Model	Accuracy	Precision	Recall	F1 Score
Random Forest	0.83	0.89	0.72	0.75
Naive Bayes	0.75	0.82	0.59	0.58
LSTM + Google News embedding	0.81	0.82	0.79	0.80
LSTM + default embedding	0.79	0.83	0.77	0.79

Table 1: Comparison of the classification metrics achieved by the developed models.

5. Conclusion

In the presented work, we have developed machine learning models that can be used to predict the name of the disease, given the drug name and the review of the drug. This will be especially helpful for users, who do not have specialized advice of medical practitioners. Also, the users, by giving names of medicine and certain reviews of the same as inputs, will be able to correctly predict the name of a disease. Thereafter, after successful matching of the observed disease and the predicted disease, the user will be able to correctly order medicines online.

We have worked with various machine learning techniques and have observed that the model, encompassing the Random Forest algorithm, gave us the best prediction results. In contrast, the deep learning models came close in terms of accuracy, but could not outperform the traditional machine learning methods, as more often than not, DL methods rely on huge amounts of data for learning patterns.

In the future, we would like to experiment with more dataset and specialized medical domain embeddings created using state-of-the-art embedding models such as BERTand RoBERTa.

References

[1] Hu, X., Gallagher, M., Loveday, W., Connor, J.P. and Wiles, J., 2015, February. Detecting anomalies in controlled drug prescription data using probabilistic models. In *Australasian Conference on Artificial Life and Computational Intelligence* (pp. 337-349). Springer, Cham.

[2] Gräßer, F., Kallumadi, S., Malberg, H. and Zaunseder, S., 2018, April. Aspect-based sentiment analysis of drug reviews applying cross-domain and cross-data learning. In *Proceedings of the 2018 International Conference on Digital Health* (pp. 121-125).

[3] Dinh, T., Detecting Side Effects and Evaluating Effectiveness of Drugs from Customers' Online Reviews using Text Analytics and Data Mining Models.

[4] Yadav, S., Ekbal, A., Saha, S. and Bhattacharyya, P., 2018, May. Medical sentiment analysis using social media: towards building a patient assisted system. In *Proceedings of the Eleventh International Conference on Language Resources and Evaluation (LREC 2018)*.

[5] Hochreiter, S. and Schmidhuber, J., 1997. Long short-term memory. *Neural computation*,*9*(8), pp.1735-1780.

American Journal of Electronics & Communication

Ankita Saha et. al., American Journal of Electronics & Communication, Vol. I (4), 22-26

A Study of Machine Learning Techniques in Cryptography for Cybersecurity

Ankita Saha[1]
Chanda Pathak[1]
Sourav Saha[2]

[1]Department of Computer Science & Engineering, Institute of Engineering and Management, Kolkata
[2]Department of Computer Science & Engineering, Kalyani University
ankitasaha.ac@gmail.com
chandapathak34@gmail.com
souravsaha1977@gmail.com

Abstract

The importance of cybersecurity is on the rise as we have become more technologically dependent on the internet than ever before. Cybersecurity implies the process of protecting and recovering computer systems, networks, devices, and programs from any cyber attack. Cyber attacks are an increasingly sophisticated and evolving danger to our sensitive data, as attackers employ new methods to circumvent traditional security controls. Cryptanalysis is mainly used to crack cryptographic security systems and gain access to the contents of the encrypted messages, even if the key is unknown. It focuses on deciphering the encrypted data as it works with ciphertext, ciphers, and cryptosystems to understand how they work and find techniques for weakening them. For classical cryptanalysis, the recovery of ciphertext is difficult as the time complexity is exponential. The traditional cryptanalysis requires a significant amount of time, known plaintexts, and memory. Machine learning may reduce the computational complexity in cryptanalysis. Machine learning techniques have recently been applied in cryptanalysis, steganography, and other data-security-related applications. Deep learning is an advanced field of machine learning which mainly uses deep neural network architecture. Nowadays, deep learning techniques are usually explored extensively to solve many challenging problems of artificial intelligence. But not much work has been done on deep learning-based cryptanalysis. This paper attempts to summarize various machine learning based approaches for cryptanalysis along with discussions on the scope of application of deep learning techniques in cryptography.

Key words: Cryptanalysis, machine learning, deep learning, ciphertext, cryptography, cybersecurity.

1. Introduction

Cryptography is the process that involves encryption and decryption of text using various mechanisms or algorithms. A cryptographic algorithm is a mathematical function that can be used in the process of encryption and decryption. Classical cryptography is the process of transforming the plain text into the ciphertext so that the data can be transmitted through some communication channels. But these communication channels are mainly insecure mediums. A data string is being used as the key which helps in the transformation of the data from plain text to cipher text. It depends on the computational complexity of the factorization of the large numbers. As the classical cryptography is solely based on mathematics, so for the manual purpose it is easy to use. The plaintexts are being protected from the casual snooping using the classical cryptography. However, the Machine Learning techniques can also be applied in cryptography. Machine learning techniques have had a long list of applications in recent years. But the use of machine learning in information and network security is not new. Machine learning and cryptography have many things in common. The most apparent is the processing of large amounts of data and large search spaces. In its varying techniques, machine learning has been an interesting field of study with massive potential for application. In the past three decades, machine learning techniques, whether supervised or unsupervised, have been applied in cryptographic algorithms, cryptanalysis, steganography, among other data-security-related applications. This paper presents an updated survey of applications of machine learning techniques in cryptography and cryptanalysis.

2. Traditional cryptography and its limitations

Traditional cryptography focuses on the sender and receiver of a known message and it uses the same secret key. In this secret key cryptography method, the sender uses the secret key to encrypt the message, and the same secret key is being used by the receiver to decrypt the message at the receiver end. Here the sender and receiver encounter the problem of agreeing on the same secret key without anyone else intercepting it. As secret-key cryptography was having difficulty regarding secure key management, public-key cryptography was invented to solve the key management problem. In public-key cryptography, a pair of keys, called the public key and the private key is provided to both the sender and the receiver. Here each person's public key is known while the private key is kept secret from both the sender and receiver. Public-key cryptography can be used for authentication as well as for encryption. Rosen-Zvi et. al.[1] proposed that the common learning in a tree parity machine can also be used as a public-key cryptosystem. It also explains that the tree parity machine has significant potential in being used as a public-key cryptosystem. But the traditional cryptography has a disadvantage of being slower. There are popular secret-key encryption methods which are significantly faster than any currently available public-key encryption method. But traditional cryptography comes at a cost

which includes time as well as money. Addition of cryptographic techniques in the information processing leads to delay. The use of public key cryptography requires setting up and maintenance of public key infrastructure requiring the handsome financial budget. Machine learning can drastically reduce the number of computational complexity regarding cryptanalysis for block ciphers and also machine learning can produce very powerful distinguishers. Elliptic curve cryptography is an alternative technique to RSA which is a powerful cryptography approach. It generates security between key pairs for public key encryption by using the mathematics of elliptic curves. Elliptic curve cryptography has gradually been growing in popularity recently due to its smaller key size and ability to maintain security. This trend will probably continue as the demand on devices to remain secure increases due to the size of keys growing, drawing on scarce mobile resources . Hashing is a method of cryptography that converts any form of data into a unique string of text. Any piece of data can be hashed irrespective of its size or type. In traditional hashing, regardless of the data's size, type, or length, the hash that any data produces is always the same length. The average user encounters hashing daily in the context of passwords. Hashing is a mathematical operation that is easy to perform, but extremely difficult to reverse. The most widely used hashing functions are MD5, SHA1 and SHA-256.

3. Machine Learning in Cryptography

Machine learning has the capability to reduce the number of computational complexity in cryptanalysis. Machine learning is basically the field of study which gives the computers the capability to learn without being explicitly trained. The process of learning begins with observations or data such as, direct experience, examples or instructions, in order to look for patterns in the data and make better decisions in the future, based on the examples that we provide. The primary aim of machine learning is to allow the computers to learn automatically without human assistance or intervention and adjust actions according to that. The basic difference between machine learning and traditional programming is, the data input and the program logic has to be fed in and then run it on the machine to get the desired output. But in machine learning, the data input and the output has been fed in and it has to be run on the machine and the machine creates its own program logic which can be evaluated while testing. Feature extraction is an important part of machine learning. It is a process of reduction of the data by selecting and combining variables into features.

R.L Rivest[2] suggested, Machine learning and cryptanalysis share many similarities. In a typical cryptanalytic situation, the cryptanalyst tries to break the complete cryptosystem or at least some parts of it. So the cryptanalyst tries to find the secret key used by the users of the cryptosystem, where the general system is already known. The main aim of cryptanalysts was to exactly identify the decryption function which was being used. This problem was described as the problem of learning an unknown function on the basis of the input/output behavior and the prior knowledge about the class of possible functions.

M.M. Alani[3] proposed different types of attacks in cryptography as well as cryptanalysis, which also showed that machine learning and cryptography share many common properties. After examining the security attacks on machine learning techniques and machine-learning-based systems, we can say that the use of machine learning techniques can be done in cryptanalysis to extract decryption keys from ciphertext blocks and also to improve their efficiency in finding solutions in the search space.

Ramani Sagar [4] proposed an overview on how AI can be applied for encrypting data and undertaking cryptanalysis of such data and other data types in order to assess the cryptographic strength of an encryption algorithm. Jonathan Blackledge et. al.[5] proposed some recent advances in the field of Cryptography using Artificial Intelligence. It specifically considered the applications of Machine Learning and Evolutionary Computing to analyze and encrypt data. It considered the implementation of Evolutionary Computing and Artificial Neural Networks for generating unique and unclonable ciphers. Al-Shammari et. al.[6] proposed a classification technique which was based on machine learning, to classify encrypted traffic. It was done to assess the robustness of machine learning classification of encrypted traffic.

4. Deep Learning in Cryptography

Deep learning is a field that is based on learning and improving on its own by examining the computer algorithms while machine learning uses simpler concepts. Deep learning works with artificial neural networks which are designed to imitate how humans think and learn. Deep learning has aided language translation, image classification and also in speech recognition. Any pattern recognition problem can be solved without human intervention using deep learning. As deep learning is a subset of machine learning, it uses a hierarchical level of artificial neural networks to carry out the process of machine learning. The hierarchical function of deep learning helps the machines to process data with a nonlinear approach. If the size of the data increases then deep learning can keep on improving. Deep learning has provided great improvements on a number of difficult tasks. Deep learning is providing great improvements in different fields day by day. Here we have studied some aspects of deep learning in different fields. The importance of cyber security is on the rise as we have become more technologically dependent than ever before. Cyber security is the state or process of protecting and recovering computer systems, networks, devices, and programs from any types of cyber attack. Cyber attacks are an increasingly sophisticated and evolving danger to our sensitive data, as attackers employ new methods powered by social engineering and artificial intelligence to circumvent traditional security controls. This paper summarizes the research done in these areas and provides suggestions for future directions in research.

Jaewoo So[7] proposed a generic deep learning based cryptanalysis model that finds the key from known plaintext-ciphertext pairs and shows the feasibility of the deep learning based cryptanalysis by applying it to lightweight block ciphers. The deep neural networks can also be used to find the key from known plaintexts. A generic and automated cryptanalysis model based on deep learning was developed and it was used for checking the safety of the lightweight block ciphers, such as S-DES, Simon, and Speck. But the drawback of the proposed DL-based cryptanalysis is that the keyspace is restricted to the text-based key. Modern cryptographic functions are designed to be very random looking and to be very complex, and therefore, machine learning is quite difficult for finding the meaningful relationships between the inputs and the outputs when the keyspace is not restricted. If the keyspace is not limited, the deep learning based cryptanalysis failed to attack the block ciphers.

Conclusion

In this paper, we have presented the survey of applications of machine learning as well as deep learning techniques in cryptography and cryptanalysis. Several studies have accounted that machine learning can significantly reduce the computational complexity regarding cryptanalysis. We have also conducted surveys on the uses of deep learning techniques on different types of cryptographic implementations. For producing more powerful cryptographic distinguisher, machine learning can be used and the resultant data and graphs from the surveys showed that the neural distinguisher achieved better accuracy and also the success rate is higher. There are lots of scopes of machine learning. It can be further used in the investment sectors, security purposes, self driving car etc. Nowadays Deep learning can also be used in these sections. These works opened ways for further research on deep learning techniques in order to get better results while challenging cryptographic implementations.

References

[1] M. Rosen-Zvi, E. Klein, I. Kanter, and W. Kinzel, "Mutual learning in a tree parity machine and its application to cryptography," Physical Review E, vol. 66, no. 6, p. 066135, 2002.

[2] "Cryptography and Machine Learning", Ronald L. Rivest, Laboratory for Computer Science Massachusetts Institute of Technology Cambridge, MA 02139.

[3] "Applications of Machine Learning in Cryptography: A Survey", MOHAMMED M. ALANI, Khawarizmi International College, United Arab Emirates.

[4] "Applications in Security and Evasions in Machine Learning: A Survey", Ramani Sagar, Rutvij Jhaveri and Carlos Borrego.

[5] "Applications of Artificial Intelligence to Cryptography", Jonathan Blackledge, Napo Mosola.

[6] R. Alshammari and A. N. Zincir-Heywood, "Machine learning based encrypted traffic classification: Identifying ssh and skype," in Computational Intelligence for Security and Defense Applications, 2009. CISDA 2009. IEEE Symposium on, pp. 1–8, IEEE, 2009.

[7] "Deep Learning-Based Cryptanalysis of Lightweight Block Ciphers", Jaewoo So Department of Electronic Engineering, Sogang University, Seoul 04107.

[8]

American Journal of Electronics & Communication

Bhuvan Agarwal et. al., American Journal of Electronics & Communication, Vol. I (4), 27-31

An API in JAVA Which Render Ease at Programming for Developers

Authors : Bhuvan Agarwal*, Soumyajeet Bhattacharjee*, Sima Kar*, Madhurima Saha*, Vijay Kumar*, Dr. Sandip Mandal*, UEM Kolkata
{Email: *sandy06.gcect@gmail.com*}

Abstract *- Based on the concept of Application programming interface (API).This project comprises of a package named "algokit" which contains several algorithms based on the category of searching, sorting, dynamic programming, tree traversals and swapping. Keeping in mind that different algorithms from the same category have its own benefit in time and space complexity, This project covers almost all the algorithms known and available from each category. This would give the user several options to choose the right algorithm for its code.An user just requires to import the package named AlgoKit and call the functions inside it for a smooth programming experience. One of the prime objectives of this project is to build a kit that serves the purpose of reducing the number of lines of code and also reduce the time taken to run the same code elsewhere. It is platform independent and can be used in any open source Java development environment.*

Keywords*: API, AlgoKi, JAVA*

INTRODUCTION

The modern era is the age of expertise and focuses on new development along with excelling in existing technologies. Today the world surrounding us is full of complex application and software. Development of these applications requires different kinds of algorithm in one project itself.

It is beneficial for developers to have an package which contains several important algorithms which is required in developing software and applications. For example-A software like Uber, which provides cab services has a very basic requirement of tracking locations on the map.

Apart from the pool of features that the software provides there must be a code for MST in that software. Keeping in mind the difficulties of a developer, Algokit is a package of algorithms which not only saves the CPU time for compiling but also saves the time and effort of a developer of explicitly writing a basic code.

LITERATURE REVIEW

Java Application Programming Interface is a library of prewritten classes.The library is divided into packages and classes. It means one can either import a single class (along with its methods and attributes), or a whole package that contains all the classes that belong to the specified package.To use a class or a package from the library,one needs to use import keyword. Similarly, this ALGOKIT is a java API that is built with all the packages and classes of sorting, searching, graphs, matrices and exception classes.

By importing this package from ALGOKIT one can get all the necessary methods and classes required.

PROPOSED WORK

Searching Algorithms: Every searching algorithm has its own best case. Focusing on that fact, here are the list of the algorithms which is present in the package.

1. Binary Search
2. Exponential Search
3. Fibonacci Search
4. Interpolation Search
5. Jump Search
6. Linear Search
7. Ternary Search

	Time Complexity
Linear Search	O (n)
Binary Search	O (log (n))
Jump Search	O (√ n)
Interpolation Search	O (log (log n))-Best | O (n)-Worst
Exponential Search	O (log (n))
Sequential search	O (n)
Depth-first search (DFS)	O (|V| + |E|)
Breadth-first search (BFS)	O (|V| + |E|)

Sorting algorithms: A comparative study of the sorting techniques based upon time complexity is discussed. Some of the sorting techniques are as follows:

1. Bubble Sort
2. Counting sort
3. Insertion sort
4. Merge sort
5. Quick sort
6. Radix sort
7. Selection sort
8. Topological sort

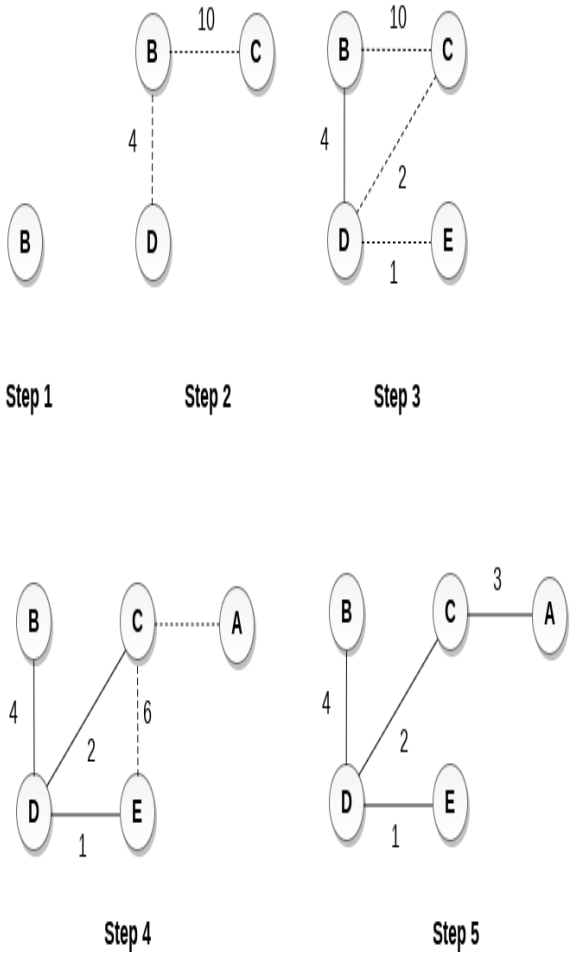
Algorithm	Time Complexity		
	Best	Average	Worst
Selection Sort	Ω(n^2)	θ(n^2)	O(n^2)
Bubble Sort	Ω(n)	θ(n^2)	O(n^2)
Insertion Sort	Ω(n)	θ(n^2)	O(n^2)
Heap Sort	Ω(n log(n))	θ(n log(n))	O(n log(n))
Quick Sort	Ω(n log(n))	θ(n log(n))	O(n^2)
Merge Sort	Ω(n log(n))	θ(n log(n))	O(n log(n))
Bucket Sort	Ω(n+k)	θ(n+k)	O(n^2)
Radix Sort	Ω(nk)	θ(nk)	O(nk)

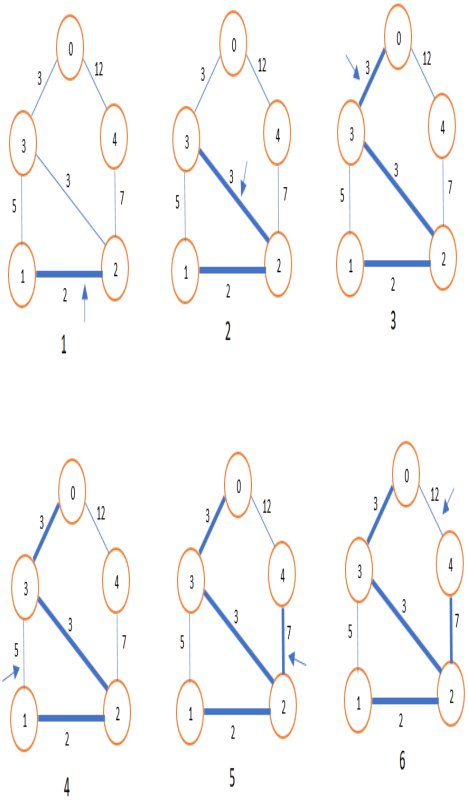
Matrix Manipulation: This topic forms a very important base for bigger graph problems and this class simple returns you the result of your matrices problems. From addition to finding Eigen values, some of the problems included are:

1. Matrix addition
2. Matrix subtraction
3. Matrix values

Graphs: MST Algorithms like Prims and krushkal returns the minimum spanning trees for a weighted, connected and undirected graph. To achieve the desired result, user only needs to give the graph as input and get the result by calling the function name like (graphs.Prims) and (graphs.Krushkal) commands respectively. Some of the graph related algorithms that this project includes are:

1. Prims
2. Krushkal
3. Dijsktras
4. DFS
5. BFS





RESULT & ANALYSIS

We have tested the algorithms implemented in ALGOKIT API with sample data and compared It with the same algorithm explicitly written in the code and found that by using ALGOKIT API the task is fulfilled in lesser lines of code thereby saving time for developers and also it makes the code more readable.

Moreover, the time taken by the code to run is also comparatively lesser than equal to when we write the whole algorithm explicitly in the code.

As every algorithm implemented under ALGOKIT API falls under one category example – algokit.search , algokit.sort , algokit.graph etc. So maintenance of such an API is also very convenient and any future changes can be made effectively.

CONCLUSION

This API contains implementation of various popular algorithms like searching , sorting , graph and matrix.It also contains several exception classes that can handle faulty data and wrong inputs. It comes in handy for developers to develop code faster just by calling these algorithms classes and its respective methods.

Thereby resulting in fewer lines of code and faster execution.

FUTURE WORK

This project will further include more algorithms on Trees and graphs that comes in handy for real world use cases. Algorithms on Trie data structure will also be included in future.

REFERENCES

[1] N. Srinivasan and A. Selvaraj, "Mobile based data retrieval using RDF and NLP in an efficient approach," *2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM),* Chennai, India, 2017, pp. 427-428, doi:10.1109/ICONSTEM.2017.8261416.

[2] Knuth, Donald (1997). "Section 6.1: Sequential Searching,". Sorting and Searching. The Art of Computer Programming. 3 (3rd ed.). Addison-Wesley. pp. 396–408. ISBN 0-201-89685-0.

[3] Thomas H. Cormen. Charles E. Leiserson. Ronald L. Rivest. Clifford Stein. Introduction to Algorithms. Third Edition. The MIT Press. Cambridge, Massachusetts.

[4] R. Boorugu and G. Ramesh, "A Survey on NLP based Text Summarization for Summarizing Product Reviews," *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, 2020, pp. 352-356,doi:10.1109/ICIRCA48905.2020.9183355.

[5] K. Nokkaew and R. Kongkachandra, "Keyphrase Extraction as Topic Identification Using Term Frequency and Synonymous Term Grouping," *2018 International Joint Symposium on Artificial Intelligence and Natural Language Processing (iSAI-NLP)*, Pattaya, Thailand, 2018, pp. 1-6, doi: 10.1109/iSAI-NLP.2018.8693001.

[6] N. Chumuang and M. Ketcham, "Model for Handwritten Recognition Based on Artificial Intelligence," *2018 International Joint Symposium on Artificial Intelligence and Natural Language Processing (iSAI-NLP)*, Pattaya, Thailand, 2018, pp. 1-5, doi: 10.1109/iSAI-NLP.2018.8692958.

[7] M. R. Hasan, M. Maliha and M. Arifuzzaman, "Sentiment Analysis with NLP on Twitter Data," *2019 International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2),* Rajshahi, Bangladesh, 2019, pp. 1-4, doi: 10.1109/IC4ME247184.2019.9036670.

[8] M. Kanakaraj and R. M. R. Guddeti, "Performance analysis of Ensemble methods on Twitter sentiment analysis using NLP techniques," *Proceedings of the 2015 IEEE 9th International Conference on Semantic Computing (IEEE ICSC 2015)*, Anaheim, CA, USA, 2015, pp. 169-170,doi:10.1109/ICOSC.2015.7050801.

*University of Engineering and Management Kolkata

American Journal of
Electronics & Communication