Evolutionary Algorithms, Fuzzy Logic and Artificial Immune Systems applied to Cryptography and Cryptanalysis: State-of-the-art review

Anjali Dadhich[#1], Dr. Surendra Kumar Yadav[*2]
[#1]*(M.tech Student) Computer Science Department,* [*2]*(Associate professor) Computer Science Department,*
JECRC University Jaipur

Abstract— **The need and importance of secure information communication, particularly text, image and video transmission has made cryptography to take a larger space in current research era. Improvement of pictorial information for betterment of human perception involves de-blurring, de-noising and safe transmission. These applications extend over several fields such as satellite imaging, medical imaging etc. Specifically we would like to elaborate our research on the significance of computational intelligence as one of the domains which finds application in cryptography and information security, and then the relevance of cryptography is indeed unavoidable.**

This paper deals with the study of the requirements for strong cryptography and various computational intelligence techniques that find use in cryptography. Cryptanalysis is a well-studied problem with many important applications in the areas of error-free and secure data transmission. In this paper, we have reviewed the improved algorithms used for cryptography optimization; the algorithms under reviews integrate genetic algorithms, immune computing, crossover and mutation operators and fuzzy systems to maintain the diversity and optimization of candidate objects. These computational intelligence techniques have seen to greatly improve the fitness levels of candidate groups in cryptography. Lastly, we make detailed comparison between these methods and those cryptography techniques without computational intelligence.

Keywords— **Cryptography, cryptanalysis, cryptosystem, evolutionary computation, decryption, encryption, computational intelligence, fuzzy logic, swarm intelligence.**

I. INTRODUCTION

In the recent years, we have witnessed significant developments in the digital information and communications technology. The computer science finds applications and pervades all areas of life, such as messaging, online shopping and education [21]. The sending and receiving of digital information is gaining importance, as the concerns related to their security and authenticity are tremendously increasing. Automatic transmission of text and images requires careful storage of data to be sent and protection from breach. Cryptography is the science which deals with ways that help us to protect and store information and transfer in a wide range and these methods depend on a secret key that is used to encrypt data [30].

As security continues to be the main issue surrounding the modern digital world, there are a lot of cyber-crimes on the rise with the development of technology. The risks involve prohibiting users from legitimate services, keep unwanted patches updated, reduced permissions and access rights of applications and users. A viable solution for this problem has been provided using cryptography. Cryptography consists of cryptology and cryptanalysis [7]. Encryption comes under cryptology and is defined as the process of converting a readable message into an unreadable form. A set of rules known encryption algorithm is used for encryption process. Newly implemented encryption algorithms have the facility to control both desired security level and the processing level, which is perceived as a great improvement for current real world applications. Various algorithms have been proposed to implement encryption in strong manners, such as statistical and probabilistic methods, Bayesian methods and computational intelligence methods. In this paper, we present a review of how computational intelligence techniques such as fuzzy logic, artificial immune systems and evolutionary algorithms contribute to design of strong cryptosystems. The use of internet and sharing the images over social networks is increasing exponentially. Provision of security to multimedia content is a major concern. Image security and encryption has become important area of research in the field of information security. Image encryption can be broadly classified into encryption with compression and encryption without compression [7] [8].

Amongst various techniques available, cryptography and cryptology benefits hugely from Artificial Neural Networks, Data Mining and Fusion, Distributed Systems, Evolutionary Algorithms, Fuzzy Systems, Knowledge Discovery, Machine Learning, Neural-Fuzzy Systems, Pattern Recognition, Reinforcement Learning and Self-Organizing Maps. Conventionally, digital data and images have been encrypted using three major steps of value transformation, pixel position permutation and formation of chaotic systems [11].

This paper structured as follows: In section 2 we discuss an overview of cryptography, cryptology schemes and cryptanalysis. Section 3 discusses various cryptographic algorithms in practice. Section 4 discusses AES and DES algorithms and their linear cryptanalysis techniques. Section 5 presents an overview of computational intelligence techniques. Section 6 presents an overview of evolutionary computation techniques and highlights particle swarm optimization applied to cryptography. Next sections discuss the application of fuzzy logic and related methods and artificial immune systems applied to cryptology. A few sections are dedicated to discussion of Dempster-Shafer theory, Hidden Markov Models and BLAST-SSAHA hybridization. We finally review the results that have been produced using application of above said techniques to cryptography and encryption and discuss their advantages and limitations. We conclude in the next section and propose some future work.

II. CRYPTOGRAPHY, CRYPTOLOGY and CRYPTANALYSIS

Cryptology is defined as the process of converting plain text to cipher text and vice versa. Cryptology deals with different varieties of cryptosystems to encrypt and decrypt the data with the use of a key [10].

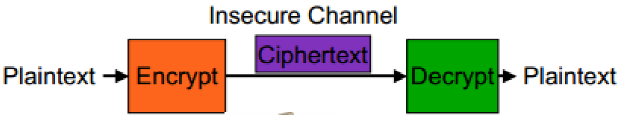


Figure 1Basic cryptology architecture

The party having a key is able to encrypt or decrypt and securely share the data among the trusted parties. The cryptographic systems can be classified as private and public key cryptosystems. In public key cryptosystem there are mainly two keys. One key is public and is shared by all the parties. Other key is private and is secret. One key encrypts and other key is meant for decrypting the cipher text. Cryptology stems from the Greek word "krypto", which means to hide, and cryptology is defined as the science of hiding [6]. Cryptography, cryptanalysis and steganography together mean secret writing. Cryptanalysis is the analyzing or breaking down of the secret codes and is the main objective under research. Decryption is to decipher what we do. Cryptology is a branch of mathematics which is implemented through lots of formal representation and with proofs about encryption as possible. Cryptography aids the issue of network security which is a broad system issue. With increase in hacking and masquerading attacks, it is concluded that the easiest way to violate security is through people. Security uses cryptology and other tools to safeguard computer users from network attacks and vulnerabilities [30].

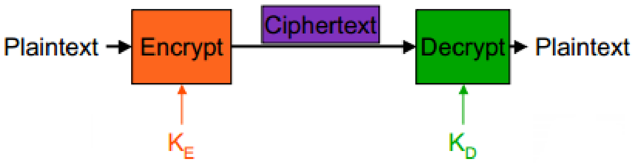


Figure 2Cryptology through key generation [6]

Cryptography always involves two things, i.e. transformation and secret. Security depends on the secrecy of the key and is assumed that the enemy can get the algorithm, can capture machines, fraud people, disassemble programs, etc. Earlier it was perceived very expensive and difficult to invent a new algorithm if the old one might have been compromised. With the use of computational intelligence, design of security algorithms has been easier and with lesser computational overhead [5].

III. OVERVIEW OF CRYPTOGRAPHIC ALGORITHMS

Three basic types of algorithms, i.e. symmetric (shared) key encryption, asymmetric (public key) encryption and secure hash functions have been popular in the domain of cryptography. For each type of algorithm, many choices are there such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blowfish, RC5, RC6 for Symmetric key encryption; RSA, El-Gamal and elliptic curve for Asymmetric key, and MD4, MD5, SHA-1, RIPEMD for secure hash functions. Different implementations within a type of algorithm share many characteristics in common, such as their goals, approaches and computational overhead required [23]. Specific implementation details may differ.

- Symmetric key encryption is an encryption technique where encryption key and decryption key are identical. The strength of algorithm is usually proportional to $2^{\text{key length}}$. This method thus assumes a truly random key and the algorithm is usually fast in execution. Around 20 cycles per byte for many algorithms is the basic achievable speed and it goes upwards towards over 100 MB/s possible on modern day processors. When implemented using hardware, it is straightforward to build hardware to run the algorithm. Decryption may be the same algorithm as encryption, but is not always required [5] [6].

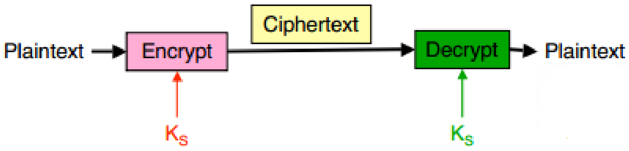


Figure 3 Symmetric-key cryptography [6]

- In asymmetric key algorithm, keys come in pairs such as: <KU, KR>, where (KU is public key and KR is private key). To strengthen the algorithm, the designation of which is public and which is private is arbitrary. Knowing one key of a pair does not let to figure out the other one. Encryption and decryption take place through the same algorithm. The keys may be applied in either order (public or private encrypt). Asymmetric key algorithm is usually much slower than symmetric key encryption with speeds achievable being much less than 1 MB/s [6].

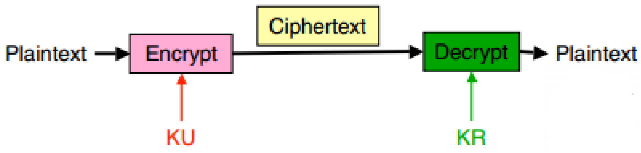


Figure 4 Asymmetric-key cryptography [6]

- Secure hash algorithms include variable-length input produces that generate a fixed-size output. Although quite similar to encryption, secure hash algorithm is without a key and output blocks collapsed together. It is more secure than asymmetric key as it is rather more difficult to construct fake plaintexts. This method suffers from weak collision resistance where it is difficult to find a plaintext with the same hash value as any randomly-chosen plaintext. This technique also offers strong collision resistance and it is difficult to find pairs of plaintexts with the same hash value. The usefulness of the method lies in the fact that secure hash function can serve as a stand-in for the plaintext for various other functions [5] [6].

Plaintext
Secure hash
Hash value

Figure 5 Secure hash algorithm [6]

There are a various other authentication and authorization algorithms pertaining to cryptography and fall under the wider umbrella of computer forensics, hash Functions, information and system integrity, internet/intranet security, intrusion detection, key/identity management, mobile communications security and network & wireless security [14].

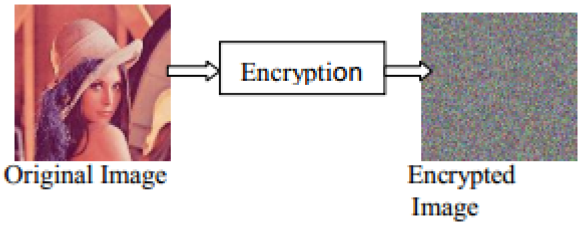


Figure 6Encryption [1]

Cryptography technique needs some algorithm for encryption of data. Nowadays when more and more sensitive information is stored on computers and transmitted over the internet, we need to ensure information security and safety. Image is also an important part of our information Therefore it is very important to protect images from unauthorized access [4].

IV. AES AND DES ALGORITHMS

A new encryption scheme has been proposed which acts as a modification of AES algorithm based on both Shift Row Transformations. In this if the value in the first row and first column is even, the first and fourth rows are unchanged and each bytes in the second and third rows of the state are cyclically shifted right over different number, else the first and third rows are unchanged and each byte of the second and fourth rows of the state are cyclically shifted left over different number of bytes [8]. Experimental result shows that this gives better encryption results in terms of security against statistical attacks and increased performance. An efficient image encryption algorithm is proposed, based on image reconstruction using some adjacent pixel characteristics. According to the different characteristics of different bit level binary images, the proposed encryption scheme reconstructs the image at the bit level [2]. Two parts of information, the significant one and the unimportant one, are treated differently and processed separately. Simulations and cryptanalysis both show that the proposed image encryption scheme is more efficient and yields better level of security [25].

Combination of Chaos And improved DES makes the final algorithm more secure, faster and more suitable for digital image encryption. Contribution of this work lies in the modification of the AES Key Expansion. The major modifications introduced are

- The initial key is expanded based on the number of pixels in the image [2].
- To improve the avalanche effect on value formed from the initial key itself [2].
- Key Expansion is done using both the s-box and Inverse s-box [2].
- Circular shift is introduced in S-box and Inverse S-box to improve the key sensitivity [2].

The encryption algorithm resulted in high encryption quality with minimal memory requirement and computational time. The key sensitivity and key space of the algorithm is very high which makes it resistant towards brute force attack and statistical cryptanalysis of original and encrypted images. The proposed technique segments the image into regions of fixed size [17]. These techniques do not hide statistical properties of the plaintext. The commonly occurring letters in plaintext result in common symbols in ciphertext and do not hide relationships in plaintext. Therefore, all natural languages become very redundant. The transmission rate is about 1.3 bits of information per letter; where many combinations of letters simply do not exist or are not common. In general, the proposed technique hides the statistical properties of the algorithm in practice [12]. This technique has been reported to encrypt a single character with a combination of 12 and 9 different symbols, with nulls, spaces and special characters at other places, thus leading to polyalphabetic ciphers. Use of different substitutions and transposition and scrambling order of letters to lead to a ciphertext-only decided how much ciphertext was optimally needed. Known plaintext often was a guess plaintext with chosen plaintext not as uncommon as it sounds. This was safe from dumpster diving but was prone to social engineering; such as rubber-hose cryptanalysis which is actually an advanced form of social engineering that uses threats, blackmail, torture, and bribery to get the key [28].

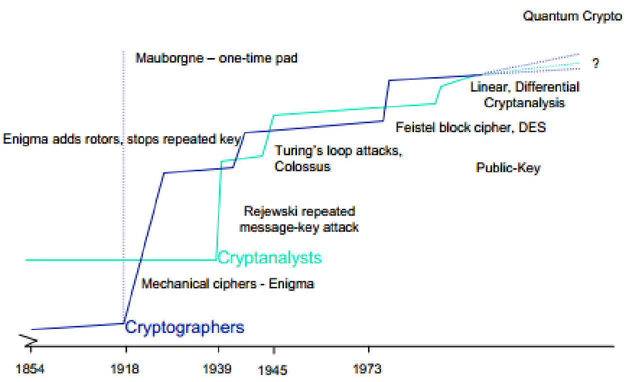


Figure 7Increasing need of cryptography [17]

V. OVERVIEW OF COMPUTATIONAL INTELLIGENCE

Numerous technological paradigms and algorithms to solve complex problems have been contrived from the studies of natural and biological systems. These algorithms are presented under the umbrella of Computational Intelligence (CI), also known as Soft Computing [8]. Considerable accomplishments have been made as a consequence of modelling biological and natural intelligence, giving rise to intelligent systems.CI is defined as "the study of the design of intelligent agents. An intelligent agent is a system that acts intelligently: What it does is appropriate for its circumstances and its goal, it is adaptable to changing environments and changing goals, it learns from experience, and it makes appropriate choices given perceptual limitations and finite computation [29]. Soft computing exhibits adaptability and an ability to learn and take care of new situations by applying reasoning, generalization, association, discovery and abstraction and does not bank on precise human knowledge. Soft Computing paradigms are basically aimed at formalizing the miraculous human ability to take rational decisions in an uncertain and imprecise environment. Whereas imprecision and uncertainty are to be avoided in hard computing, these are exploited in soft computing to arrive at a decent solution [13]. The most popular and frequently used soft computing paradigms include Artificial Neural Networks (ANN), Evolutionary Computation (EC), Artificial Immune Systems (AIS), Swarm Intelligence (SI) and Fuzzy Logic (FL) [26].

Computational Intelligence represents a set of nature inspired computational methodologies and approaches to address complex problems of the real world applications to which traditional methodologies and approaches are ineffective. These methods have found a variety of applications in the field of optimization problems. Some of those applications belong to the area of information security. First research papers dealing with the subject appeared in 1979 and presented cryptanalysis of simple substitution cipher by means of relaxation algorithms [10]. Since then, as problem solving techniques in information security, several areas of biologically inspired computation methods that belong to computational intelligence gained attention. Although in this paper we limit our research to fuzzy sets, evolutionary computation methods and immune systems, it is justified to mention several others, like artificial neural networks, DNA computing, and cellular automata as possible alternatives [19].

In the field of cryptography and secure key generation we come to the conclusion that to generate secure keys and to encrypt data, there are multiple approaches [9] [18] [20]. Some of them are listed as follows:

- Fusion Approach Using Dempster-Shafer Theory and Bayesian Learning
- Blast-Ssaha Hybridization
- Hidden Markov Model
- Neural Network
- Bayesian Network
- Genetic Algorithm
- Artificial Immune System
- K- nearest neighbor algorithm
- Support Vector Machine
- Decision Tree
- Fuzzy Logic Based System
- Meta Learning Strategy

VI. EVOLUTIONARY COMPUTATION APPLIED TO CRYPTOGRAPHY

Evolutionary Computation methods use iterative progress, such as growth or development in a population. This population is then selected in a guided random search to achieve the desired goal. Such processes are often inspired by biological mechanisms of evolution. Genetic algorithm is a search heuristics that mimics the process of natural evolution. Genetic algorithms are based on the Darwinian theory of evolution. Genetic algorithms have been invented by J. Holland in 1960s, and since then they have been successfully applied to the variety of problems in the field of cryptography and key detection using combinatorial optimization [5]. Because of their popularity, numerous variations of genetic algorithms have been developed since their invention. In genetic algorithms, the population of individuals which represent possible solutions to an optimization problem evolve toward a better solution. To measure the quality of a solution, the fitness function is defined. A fitness function is always problem dependant. The evolution in genetic algorithm usually starts from a pool of randomly selected individuals and then, by utilizing the GA operators, a new and better population is generated. Main genetic algorithm operators are selection, crossover, and mutation. Selection is a process of selecting individuals that will produce a new generation. Crossover works by combining two or more parent solutions to form one or more solutions that have their good characteristics. Mutation is a random change of individual alleles in an individual [20] [24]. Genetic programming represents evolutionary methodology inspired by biological evolution to find computer programs. They are used to optimize a population of computer programs according to a fitness landscape. Evolutionary computation algorithms represent a range of problem-solving techniques based on principles of biological evolution, like natural selection and genetic inheritance [21]. Such algorithms can be used to solve a variety of difficult problems, among which are those from the area of cryptography. Examples of such an approach include the evolving hash functions or creation of a new block cipher. First results in this area have emerged over 30 years ago, and in recent years there has been an increased interest in this area. Still, some problems like problem formulation and representation remain open. The purpose of this paper is to give a survey of cryptographic applications that can be developed with the help of evolutionary computation methods, and to address their applicability to the real-world scenarios [20].

VII. FUZZY SET THEORY APPLIED TO CRYPTOGRAPHY

A. Fuzzy Neural Network: The aim of FNNs in cryptography and secure key generation is to process the massive volume of uncertainty in data and image information, which is wide-spread in our life [19]. [28] propose fuzzy neural networks on parallel machines to speed up rule production for public-key and private-key generation, customer-specific image data sets and intermediate fraud detection [4].

B. Fuzzy Darwinian System: Fuzzy Darwinian Detection [13] is Evolutionary-Fuzzy system which uses genetic programming for evolving fuzzy logic rules. It classifies the transactions into suspicious and non-suspicious. It comprises of Genetic Programming (GP) search algorithm and a fuzzy expert system. This approach has very high accuracy and produces a low false alarm. But it is not applicable to online data transfer transactions and in decryption it takes a lot of time. Also it is highly expensive and processing speed is low [18].

Fuzzy logic is the branch of logic in which the truth value of a logical proposition (or variable) is represented as a real value on unit interval [0,1]. Fuzzy logic is a problem-solving control system methodology that presents itself to implementation in systems ranging from simple, small, embedded micro-controllers to large, networked, multi-channel PC or workstation-based data acquisition and control systems. Fuzzy logic provides a simple way to arrive at a definite conclusion based upon vague, ambiguous, imprecise, noisy, or missing bits of information. In fuzzy logic rules and membership sets are used to make a decision. To achieve security and low processing, the algorithm uses variable keys. Fuzzy logic is the system of logical reasoning where the options are not binary but instead the truth value is part of a continuum on the interval from Certainly False (Zero) and Certainly True (One). Fuzzy logic is different than the binary logic of Aristotle. For example the Aristotle's Law of the Excluded Middle is not true under fuzzy logic. An item can simultaneously be both somewhat Tall and somewhat Not Tall. If I am 2 meters tall, my Tallness varies depending on whether I am among horse jockeys or NBA players. Within the discipline of fuzzy logic there is some dispute as to on the nature of the truth value [23]. Some contend the truth value of fuzzy variable is strictly the probability the proposition is true or not. This is uncertainty. Others contend concepts such as vagueness and ambiguity can be model by fuzzy logic but are separate and distinct from simple probabilistic uncertainty [12].

VIII. FUSION APPROACH USING DEMPSTER-SHAFER THEORY AND BAYESIAN LEARNING

Dempster-Shafer theory basically proposes cryptography and cryptanalysis of 4-rouund and 8-round DES and AES algorithms. It proposes an NP-hard detection system using information fusion and Bayesian learning in which evidences from current as well as past behavior are combined together and depending on certain type of decryption and key-recovery behavior establishes an activity profile for every cardholder [1]. It has advantages such as:- high accuracy, processing speed, reduced false alarms, improved detection rates and key-generation rates, applicability in strong cryptanalysis. But one disadvantage of this approach is that it is highly expensive. Fig. shows the block diagram of the linear cryptanalysis of 4-round DES algorithm. Dempster–Shafer theory and Bayesian learning is a hybrid approach for linear cryptanalysis [18][19][20] which combines evidences from current as well as past behavior.

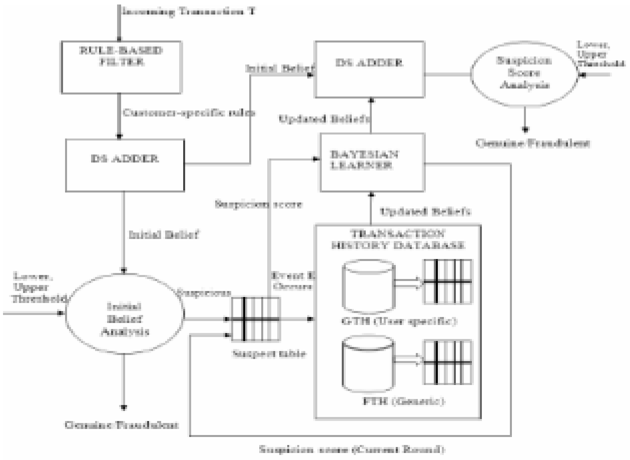


Figure 8 Fusion Approach Using Dempster-Shafer Theory And Bayesian Learning [20]

Every key-generation, transmission and recovery has a certain type of substitution, transposition and modulo-2 behavior associated with it, which establishes an activity profile for each key. This approach proposes a false key reporting system using information fusion and Bayesian learning so as to counter false key generation or unauthorized key recovery. The system consists of four components, namely, rule-based filter, Dempster–Shafer adder, key transmission history database and Bayesian learner. In the rule-based component, the substitution and transposition level of each transmitted key based on the extent of its deviation from good pattern is determined [9]. Dempster–Shafer's theory is used to combine multiple such evidences and an initial belief is computed [5]. Then the initial belief values are combined to obtain an overall belief by applying Dempster-Shafer theory. The transaction is classified as perfect key-generation and recovery depending on this initial belief. Once a weak cryptanalysis is found, belief is further strengthened or weakened according to its similarity with other weak cipher generation history using Bayesian learning [8]. It has high accuracy and high processing Speed. It improves detection rate and reduces false alarms and also it is applicable to strengthen RSA algorithm. But it is highly expensive and its processing speed is low [17].

IX. BLAST-SSAHA HYBRIDIZATION

As the name suggests, Blast-Ssaha Hybridization [11] is a hybridization of BLAST and SSAHA algorithms which is referred as BLAH-FDS algorithm. This algorithm is basically the efficient two-stage sequence alignment algorithm which is used for analyzing key-recovery patterns, both legitimate and through brute-force or other attacks. The performance of this algorithm is good, also accuracy is high. It is useful in telecommunication and MD-5 secure hash schemes and processing speed is also high. But disadvantage is that it does not detect cloning of ciphers [18].

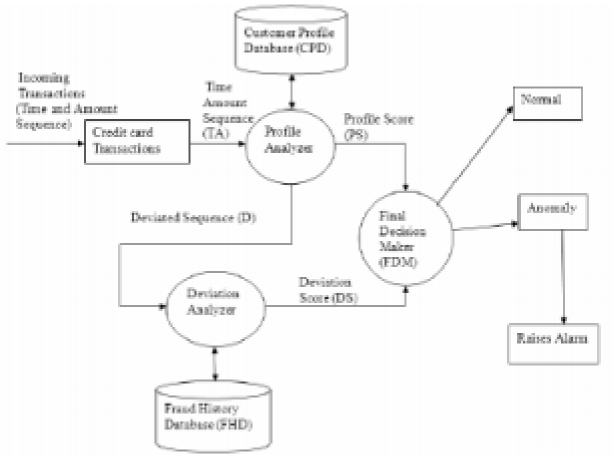

Customer Profile Database (CPD)
Incoming Transactions (Time and Amount Sequence)
Credit card Transactions
Time Amount Sequence (TA)
Profile Analyzer
Profile Score (PS)
Normal
Deviated Sequence (D)
Final Decision Maker (FDM)
Anomaly
Deviation Analyzer
Deviation Score (DS)
Raises Alarm
Fraud History Database (FHD)

Figure 9 BLAST-SSAHA Hybridization for Cryptology Applications [18]

X. HIDDEN MARKOV MODEL

A Hidden Markov Model is a double embedded stochastic process widely used to model much more complicated stochastic processes as compared to a traditional Markov model. In cryptology applications, if a transmitted key is not accepted by the trained Hidden Markov Model with sufficiently high probability, it is considered to be a brute force or a similar cryptanalysis attack. Baum Welch algorithm is used for training purpose and K-means algorithm for clustering. HMM sores data in the form of clusters depending on three key-length value ranges, viz. low, medium and high [10]. The probabilities of initial set of key lengths, complete or partial are chosen and checks are performed whether the recovered key bit can be accessed only by the intended recipient or by the hacker. Since HMM maintains a log for transactions it reduces tedious work of employee but produces high false alarm as well as high false positive[4]. A Hidden Markov Model is a double embedded stochastic process which is used to model much more complicated stochastic processes as compared to a traditional Markov model. If a supposed key length and generation pattern is not accepted by the trained Hidden Markov Model with sufficiently high probability, it is considered to be a weak key. A Hidden Markov Model [23] is initially trained with the normal cryptanalyst behavior. It works on the various key transmissions, ciphertext generation and decryption profiles which can be divided into three types such as 1) Lower profile; 2) Middle profile; and 3) Higher profile [9]. The use of chaotic maps to construct dynamic S-Box has been increasingly studied. Dynamic chaotic S-Boxes enhance the security criteria of the block ciphers. HMM based S-Boxes are based on the combination of two chaotic maps: one and three dimensional piecewise linear maps. The randomness of these maps seems to be crucial to keep the randomness and the uniformity of the binary sequences. The security analysis shows that the dynamic S-Boxes based on two chaotic maps have the lowest linear approximation probability [2] [3].

XI. OVERVIEW OF ARTIFICIAL IMMUNE SYSTEMS IN CRYPTOGRPHY

Error correcting codes and cryptography have benefitted immensely from Artificial Immune Systems (AIS), derived from human immune systems (HIS). AIS is a multilayered defense system comprising of cells and molecules which interact in various ways to detect and eliminate infectious agents (pathogens) from our body. AIS differentiates between self, (S), and (ii) non-self (NS) peptides and then assigns the right effectors to eliminate each pathogen. Similarly, AIS can be used as an anomaly detection system which sets apart fraudulent and weak ciphertexts from genuine ones. The input for the AIS based cryptology system is the key generation algorithm, and cryptanalysis survival report of the resulting ciphertext [30]. The AIS analogy helps to promote e-commerce as it will effectively minimize losses due to weak-ciphers and other cryptanalysis attacks. AIS make cryptanalysis and 4-round DES algorithms more robust by incorporating immune features such as affinity maturation and somatic hyper-mutation in the future. AIS act as parallel adaptive information-system (IS) which works on the principle of simple and, localized rules. AIS interacts with pathogens in a localized fashion. Surfaces of AIS cells are covered with receptors, which chemically bind to (i) pathogens, and (ii) other immune system cells or molecules. Also AIS cells circulate around the body via the blood and lymph systems, forming a dynamic system of distributed detection and response [24]. AIS has no centralized control, and hierarchical organization, thus responding to ciphers and ciphertexts in robust manner [30].

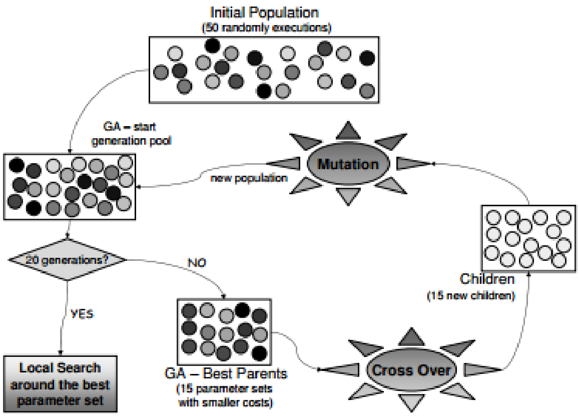
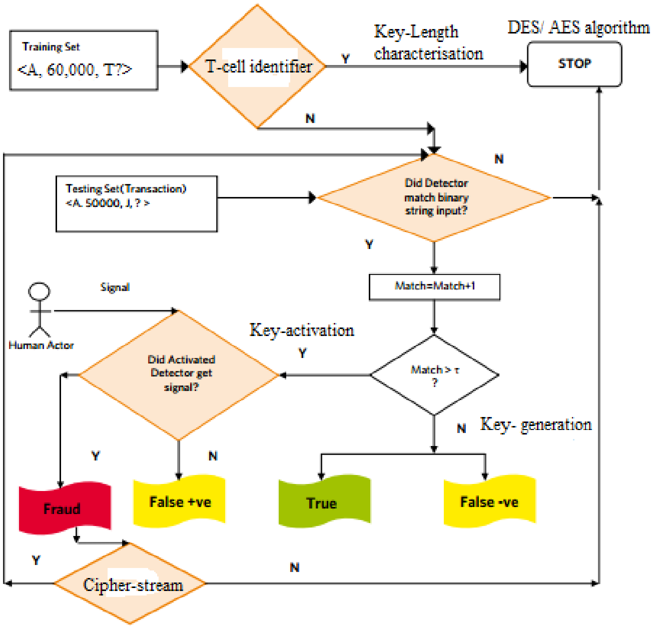


Figure 10Artificial Immune Systems basics [30]

AIS detectors can be mobile agents that migrate across networks of cryptanalysts, and key-generation algorithms. It has been shown that the optimal computation of finite field exponentiation is a problem which is closely related to finding a suitable addition chain with the shortest possible length [25]. However, it is also known that obtaining the shortest addition chain for a given arbitrary exponent is an NP-hard problem. As a consequence, heuristics are an obvious choice to compute field exponentiation with a semi-optimal number of underlying arithmetic operations [30]. The use of an artificial immune system is efficient to tackle this problem. Particularly, the problem of finding the shortest addition-chains for exponents with moderate size spanning a length of less than 20 bits, and for the huge exponents typically adopted in cryptographic applications, (i.e., in the range from 128 to 2048 bits) [25].



(T=True. F=Fraud: A. C=Source of transaction: 50000. 60000=Amount. B. D. J= Destination)

Figure 11 AIS architecture for cipher-text generation [25]

XII. DATA AND IMAGE ENCRYPTION USING COMPUTATIONAL INTELLIGENCE

Data communication is transmission data from a point to another. Nowadays main issue in data communication is the security. Encryption offers a viable solution to this problem. The encryption algorithm is the mathematical process for performing encryption on data [1]. The proposed algorithm supports for user desired security level and processing level. The algorithm provides security levels and their corresponding processing levels by generating random keys for the encryption/decryption process. This facility is achieved efficiently and effectively using computational intelligence tools. In this section, the results of the proposed encryption algorithms using various computational intelligence techniques have been analyzed by comparing with other existing encryption algorithms. The aim of the research is to examine the effectiveness of computational intelligence tools in cryptography and to encourage building new algorithms using requirements which will be more advanced than the existing encryption algorithms. Most cryptographic primitives (e.g. bit, byte, bitwise operators, logical operations, substitution, permutation, addition, etc) can be imparted the concept of a fuzzy bit. The truth value of a fuzzy bit is the Bayesian probability that the bit is set (equal to 1). Building up from a single fuzzy bit, various cryptographic primitives needed to implement the DES and AES algorithms have been using fuzzy bits throughout [4] [7].

This gives rise to a powerful new approach to cryptanalysis because quantitative measures of confusion, diffusion, and avalanche can be obtained. With such measurements it is now possible to quantitatively compare the cryptographic features of various algorithms [9]. The general scheme was to carefully track the flow of information as it was transformed by various cryptographic primitives. In a known text attack the input and output texts are known with perfect certainty. By setting all of the bits of the key to perfect uncertainty (truth value is equal 1), one could set and clear each bit of the key in succession. For each of the 2N keys where only 1 bit is known with certainty, the cryptographic algorithm is applied to the perfectly known input to produce an output where each output bit has a value in the real interval [0,1]. The set of fuzzy bits could then be compared to the expected output [15]. The value of this comparison is the probability the vector of fuzzy bits is equal to the expected output bits. From these comparisons, it was found that based on the fuzzy output, we could find an output which was “closest” to the expected output; with a single bit of the key could then be set or cleared [16]. Once one bit is clear the process would be repeated where each possible second key bit is set or cleared in succession.

For the practitioners of genetic-fuzzy sets, the truth value of a fuzzy variable is different than the value derived using Bayesian probability theory. Cryptography admits only one form of fuzzy; probabilistic uncertainty. A bit in a cryptographic system is either 1 or 0. We are uncertain which value is the correct value of the bit, but there is one and only one correct value. Uncertainty of this form is correctly modelled by Bayesian probability theory [16]. A fuzzy bit for the purposes of cryptanalysis is a binary bit where the value of the bit may be uncertain. But, this is an area for future research because the mathematic for the predicate logic of pure fuzzy logic is simpler than that of probability. It is possible the same results can be had from fuzzy cryptanalysis with a significantly lower computational cost [15].

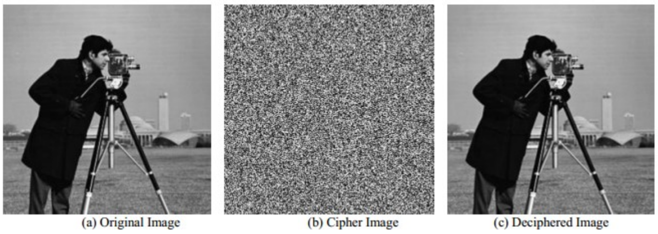

(a) Original Image (b) Cipher Image (c) Deciphered Image

Figure 12Encryption and decryption obtained using evolutionary computation and swarm intelligence [21

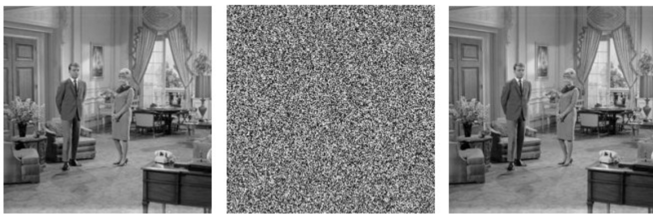


Figure 13Encryption and decryption obtained using Fuzzy Logic [26]

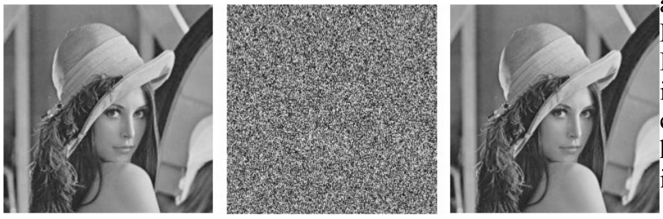


Figure 14 Encryption and decryption obtained using Artificial Immune Systems [25]

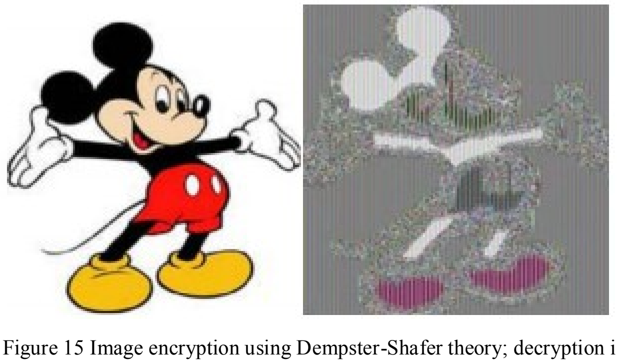


Figure 15 Image encryption using Dempster-Shafer theory; decryption is an expensive process using this method [7]

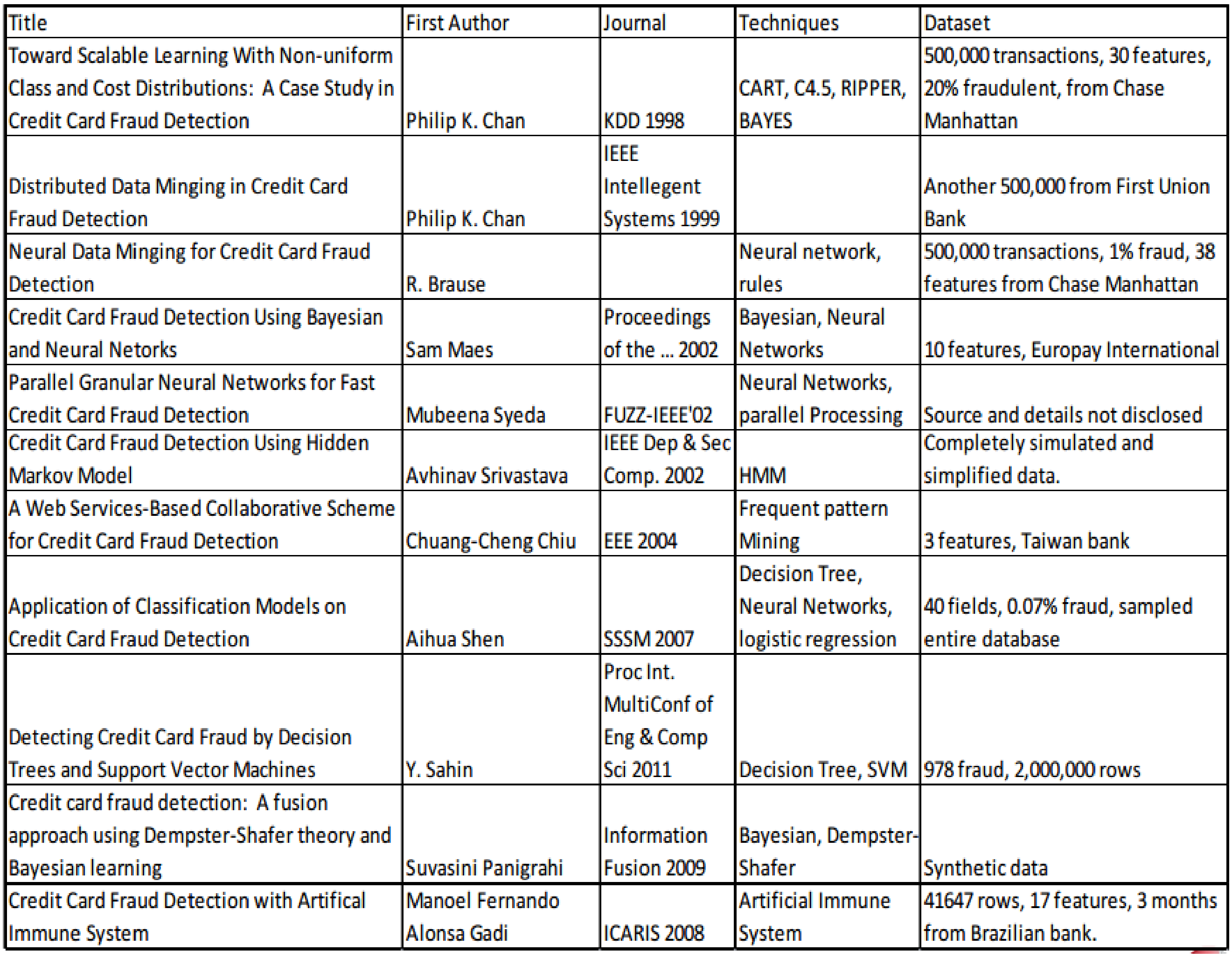
XIII. REVIEW OF RESULTS

Vision processing incorporates human perception and intelligence which makes the field most interesting to the research community as it can mimic human behaviour in the computer system by means of video surveillance system, integrating more intelligence to machines such as robots, as well as in ecology, biometrics and medical applications. This leads to a secure communication channel, transmitted images also need to be processed exhaustively to find out any vital information about ciphertexts [21]. With the ever-increasing growth of multimedia applications, security is an important issue in communication and storage of images, and Encryption is a common technique to uphold image security. Image encryption techniques try to convert original image to another image that is hard to understand; to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption [23]. The process of encoding plain text messages into cipher text messages is called encryption and the reverse process of transforming cipher text back to plain text is called as decryption. Image and video encryption have applications in various fields including internet communication, multimedia systems, medical imaging, Tele-medicine and military communication [18]. Colour images are being transmitted and stored in large amount over the Internet and wireless networks, which take advantage of rapid development in multimedia and network technologies. In recent years, plenty of colour image encryption approaches have been proposed. Until now, various data encryption algorithms have been proposed and widely used, such as AES, RSA, or IDEA most of which are used in text or binary data. It is difficult to use them directly in multimedia data and inefficient for colour image encryption because of high correlation among pixels. For multimedia data are often of high redundancy of large volumes and require real-time interactions [6].

XIV. ANALYSIS AND COMPARISON OF PSS-PSO TECHNIQUE

It has become relatively comprehensible to deal with the balance between cipher-exploitation and new cipher-pattern exploration. Exploration is the ability to test various regions in the problem space in order to locate a good optimum, hopefully the global one, and exploitation is the ability to concentrate on the search around a promising candidate solution in order to locate the optimum precisely [13]. Fast convergence velocity tends to result in the premature solution as opposed to the best solution. The predatory search strategy (PSS) to solve cryptology problems in particular have assisted to solve discrete variable optimization problems. This strategy is an individual-based searching strategy and has a good balance between exploitation and exploration. On a general note, the balance of exploitation and exploration is not only a key problem for discrete variable optimization problems but also for the continuous variable optimization problems [27]. Researchers have attempted to integrate the PSS with swarm intelligence techniques to solve continuous variable optimization problems in cipher text generation and secure cryptanalysis. Particle Swarm Optimisation (PSO) is adopted to be incorporated with the PSS. Compared with well-known PSO algorithms, the PSS-PSO is found to achieve a superior performance to the existing algorithms for continuous variable optimization problems. The following table presents the related works of PSS and PSO algorithms and outlines the advantages offered by the basic idea of PSS-PSO and discusses the benefits of implementation of the PSS-PSO approach [20].

Table 1 Comparison of performance of various credit card detail encryption schemes, implemented using Fuzzy Logic, Artificial Immune Systems, Artificial Neural Networks and Evolutionary Algorithms [7] [12] [17] [19] [22] [28]



Title	First Author	Journal	Techniques	Dataset
Toward Scalable Learning With Non-uniform Class and Cost Distributions: A Case Study in Credit Card Fraud Detection	Philip K. Chan	KDD 1998	CART, C4.5, RIPPER, BAYES	500,000 transactions, 30 features, 20% fraudulent, from Chase Manhattan
Distributed Data Minging in Credit Card Fraud Detection	Philip K. Chan	IEEE Intellegent Systems 1999		Another 500,000 from First Union Bank
Neural Data Minging for Credit Card Fraud Detection	R. Brause		Neural network, rules	500,000 transactions, 1% fraud, 38 features from Chase Manhattan
Credit Card Fraud Detection Using Bayesian and Neural Netorks	Sam Maes	Proceedings of the ... 2002	Bayesian, Neural Networks	10 features, Europay International
Parallel Granular Neural Networks for Fast Credit Card Fraud Detection	Mubeena Syeda	FUZZ-IEEE'02	Neural Networks, parallel Processing	Source and details not disclosed
Credit Card Fraud Detection Using Hidden Markov Model	Avhinav Srivastava	IEEE Dep & Sec Comp. 2002	HMM	Completely simulated and simplified data.
A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection	Chuang-Cheng Chiu	EEE 2004	Frequent pattern Mining	3 features, Taiwan bank
Application of Classification Models on Credit Card Fraud Detection	Aihua Shen	SSSM 2007	Decision Tree, Neural Networks, logistic regression	40 fields, 0.07% fraud, sampled entire database
Detecting Credit Card Fraud by Decision Trees and Support Vector Machines	Y. Sahin	Proc Int. MultiConf of Eng & Comp Sci 2011	Decision Tree, SVM	978 fraud, 2,000,000 rows
Credit card fraud detection: A fusion approach using Dempster-Shafer theory and Bayesian learning	Suvasini Panigrahi	Information Fusion 2009	Bayesian, Dempster-Shafer	Synthetic data
Credit Card Fraud Detection with Artifical Immune System	Manoel Fernando Alonsa Gadi	ICARIS 2008	Artificial Immune System	41647 rows, 17 features, 3 months from Brazilian bank.

As mentioned, PSO is a population-based search algorithm that is applied over a population of individuals and returns a region of the function space with best possible solution. The population is known as the swarm and the individual entities are termed as particles [3]. Each particle is moved in the search space at an adaptive velocity. Each particle is clustered into a neighbourhood that consists of a specific number of particles. Each particle retains the best position it went through in its memory. Finally, the best position encountered by all the particles is communicated to each particle of the swarm [6].

XV. CONCLUSION & FUTURE SCOPE

In this paper, we have analyzed how various computational and artificial intelligence techniques can be applied to cryptography. Their advantages in various domains of cryptography such as key-generation, secure transmission, image encryption and cryptanalysis have been studied. It has been found that the bit picking scheme for recovering the cryptographic key of a known text pair was quite successful with fuzzy logic and artificial immune systems. The research proved useful even with some failures as it was illuminating to observe and document the introduction and spread of uncertainty in a cryptographic system. This gives rise to possibility to more precisely quantify the information theory concepts, confusion and diffusion. Such precision provide the opportunity to use fuzzy cryptanalysis to construct better cryptograph better cryptographic primitives such as S-Boxes. It also allows for demonstration and measurement of the strength or weakness of various cryptographic systems. There seems to be no restriction to applying evolutionary algorithms, Dempster-Shafer theory and fuzzy cryptanalysis to various areas of cryptographic research such as encryption, linear cryptanalysis transfer protocols or blinding protocols.

Currently, strong key generation and secure transmission, and to withstand cryptanalysis attacks is one of the key tasks. There are many ways of detection of key-hacking, brute force, and cipher text misuse. If one of these or combination of algorithm is applied into cryptology, the probability of strong key retention and secure DDES can be predicted soon after encryption. A series of anti-cipher strategies can be adopted to prevent data loss and reduce risks. This paper gives contribution towards the effective ways of cipher text generation, handling and image encryption.

References

[1] Abhinav Srivastava, Amlan Kundu, Shamik Sural and Arun K. Majumdar, "CreditCard Fraud Detection Using Hidden Markov Model" IEEE, Transactions On Dependable And Secure Computing, Vol. 5, No 1. , January-March 2008.

[2] Albassall A.M.B., Wahdan A.: Genetic Algorithm cryptanalysis of a Fiestal type block cipher. Proceedings of ICEEC '04, pp. 217-221 (2004).

[3] Ali Aydın Selçuk.: On Probability of Success in Linear and Differential Cryptanalysis. In J. Cryptology Vol. 21, pp. 131–147 (2008).

[4] Amlan Kundu, Suvasini Panigrahi, Shamik Sural and Arun K. Majumdar, "Credit card fraud detection: A fusion approach using Dempster-Shafer theory and Bayesian learning," Special Issue on Information Fusion in Computer Security, Vol. 10, Issue no 4, pp.354- 363, October 2009.

[5] B. Carter and T. Magoc.: Classical Ciphers and Cryptanalysis. Technical Report (2007).

[6] Bárbara E. Sánchez Rinza, Diana Alejandra, Bigurra Zavala, Alonso Corona Chavez.: De-encryption of a text in spanish using probability and statistics. In proceedings of 18th International Conference on Electronics, Communications and Computers IEEE 2008, pp 75-77 (2008).

[7] Carlisle Adams.: Designing against a class of algebraic attacks on symmetric block ciphers. J. Applicable Algebra in Engineering, Communication and Computing Vol. 17, pp. 17–27 (2006).

[8] Eberhart, R.C. and Kennedy, J. (2001) Swarm Intelligence. London: Morgan Kauf-mann Publishers.

[9] Engelbrecht, A.P. (2007) Computational Intelligence: An Introduction. 2nd ed. Chichester : Wiley.

[10] K.W. Lee, C.E. Teh, Y.L. Tan.: Decrypting English Text using enhanced frequency Analysis. In proceedings of National Seminar on Science, Technology and Social Sciences 2006 pp. 1-7 (2006).

[11] Laskari, E. C., Meletiou, G. C., Stamation, Y. C., and Vrahatis, M. N., Evolutionary Computation based Cryptanalysis: A first study. Nonlinear Analysis, vol. 63, no.(5- 7), pp. 823-830, 2005.

[12] Linda Delamaire (UK), Hussein Abdou (UK), John Pointon (UK), “Credit card fraud and detection techniques: a review”, Banks and Bank Systems, Volume 4, Issue 2, 2009

[13] M.S.V.S. Bhadri Raju, Effect of Language complexity on Deciphering Substitution Ciphers - A case study on Telugu. International Journal of Security and its applications (IJSIA), Vol. 4, Issue 1, Science and Engineering Research Society (SERSC), Korea, pp. 11-20 (2010).

[14] Michael J. Wiener.: The Full Cost of Cryptanalytic Attacks. J. Cryptology Vol. 17, pp 105–124 (2004).

[15] R, Vimalathithan., and Valarmathi, M. L., Cryptanalysis of S-DES using Genetic Algorithm”. International Journal of Recent Trends in Engineering, vol. 2, no. 4, pp.76-79, Nov. 2009.

[16] Ruth M. Davis, The Data Encryption Standard, Proceedings of Conference on Computer Security and the Data Encryption Standard, National Bureau of Standards, Gaithersburg, MD, Feb. 15, 1977, NBS Special Publication 500-27, pp. 5-9.

[17] Sam Maes, Karl Tuyls, Bram Vanschoenwinkel, Bernard Manderick,"Credit card fraud detection using Bayesian and neural networks,"Interactive image-guided neurosurgery, pp.261-270, 1993.

[18] Sandeep Pratap Singh, Shiv Shankar P.Shukla,Nitin Rakesh and Vipin Tyagi "Problem Reduction In Online Payment System Using Hybrid Model" International Journal of Managing Information Technology (IJMIT) Vol.3, No.3, August 2011.

[19] Sean Simmons, Algebraic Cryptanalysis of Simplified AES. In J. Cryptologia, Vol. 33, pp 305–314 (2009).

[20] Seung-Jo Han, The Improved Data Encryption Standard (DES) Algorithm, pp. 1310-1314 (1996).

[21] Shahzad, W., Siddiqui, A. B., and Khan, F. A., Cryptanalysis of Four-Round DES using Binary Particle Swarm Optimization. Genetic and Evolutionary Computation Conference, pp. 1757-1758, July 8-12, (2009).

[22] Song, J., Zhang, H., Meng, Q., and Wang, Z., Cryptanalysis of Four-Round DES Based on Genetic Algorithm. International Conference on Wireless Communications Networking and Mobile Computing, Issue 21-25, pp. 2326-2329. (2007).

[23] Stallings, W. Cryptography and Network Security Principles and Practices. Pearson Education, (2004).

[24] Subbarao V. Wunnava, Data Encryption Performance and Evaluation Schemes, Proceedings IEEE Southeast conference, pp. 234-238. (2002)

[25] Sujith Ravi and Kevin Knight.: Attacking Decipherment Problems Optimally with Low-order N-gram Models. In proceedings of the conference on Empirical Methods in Natural Language Processing, pp. 812-819 (2009).

[26] Sujith Ravi, Kevin Knight.: Attacking Letter Substitution Ciphers with Integer Programming. In J. Cryptologia Vol. 33, Issue 4, pp. 321-334, (2009).

[27] Toemer, R., and Arumugam, S. Breaking Transposition Cipher with Genetic Algorithm. Electronics and Electrical Engineering. vol.7 no.79, pp.75 – 78. (2007).

[28] Uddin, M. F., and Youssef, A. M. Cryptanalysis of simple substitution cipher using Particle Swarm Optimization. IEEE Congress on Evolutionary Computation, pp. 677-680, 2010.

[29] V.Bhusari ,S.Patil ," Study of Hidden Markov Model in Credit Card Fraudulent Detection ",International Journal of Computer Applications (0975 - 8887) Volume 20- No.5, April 2011.

[30] Z. Lin and H. Wang, “Efficient image encryption using a chaos-based PWL memristor,” IETE Technical Review, vol. 27, no. 4, pp. 318–325, 2010.